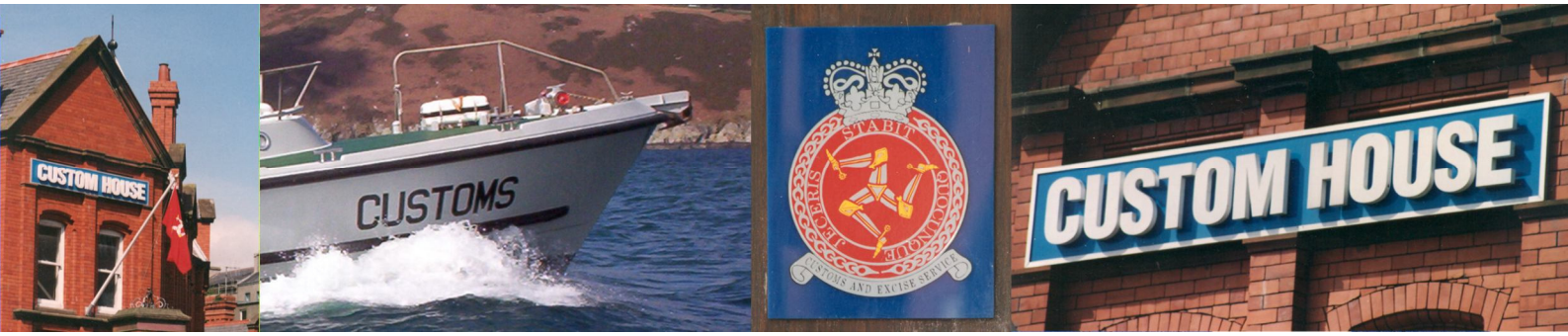
Treasury
Customs and Excise Division

Notice 1000 MAN

Trade-Based Money Laundering



August 2015
(updated to 10 March 2021)

Isle of Man Government
Reiltys Ellan Vannin

Important Notice

This Notice is not intended as an authoritative statement of the law. It is intended to provide a general overview of the risks and challenges associated with trade-based money laundering and what might be done to prevent and combat it.

Index

Isle of Man Government

Reiltys Ellan Vannin

1. **What is trade-based money laundering ("TBML")?**

FATF has identified three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origin and to integrate it into the formal economy. These methods involve -

a. the use of the financial system (or by use of the informal economy - by such means as *hawala*);

b. the physical movement of cash such as by the use of cash couriers; and

c. what may be described in general terms as "trade-based money laundering".

Whilst the first two of these methods have received considerable attention, the third has not been subject to as much scrutiny nor has there been as much guidance provided.

TBML may be seen as the process of either (or both) -

- disguising the proceeds of crime; and

- moving its value using the cover of real or concocted trade transactions,

so as to legitimise the illicit origins of the proceeds.

These processes could involve -

a. misrepresenting the price, quality or quantity of goods being bought and sold, transported, imported, exported or otherwise traded;

b. creating a partly or wholly bogus trading arrangement, or trading pattern, that can be used to justify the movement of value from one place or person to another (sometimes referred to as "phantom shipping"); or

c. diversion of the goods from their original, stated destination back into the country of origin to avoid taxes or duties, for sale on the black market or insertion into the legitimate supply chain. Sometimes referred to as "U-Boat shipping", it has been seen in the UK in excise diversion fraud of alcoholic drinks, for example.

TBML is often used in conjunction with other money laundering techniques, so as to make detection more difficult.

TBML might involve fraud by one party against another, but equally it can also depend on there being some element of collusion between the seller and buyer, given that the intention is to have in use an apparent value in excess of what would be expected from an arms' length transaction, or for the funds involved to be transferred without being detected by the authorities. The collusion may arise because the parties are controlled by the same persons, or because one or both of the parties are attempting to evade taxes (such as in so-called "carousel" or "MTIC" VAT fraud) on some part of the transaction.

The International Chamber of Commerce has also highlighted the use of some of the techniques of TBML by otherwise legitimate businesses to avoid (or evade) taxes, or to avoid currency controls imposed in one or more of the countries involved in a transaction.

Studies undertaken by FATF have concluded that TBML represents an important channel of criminal activity, and is increasingly important given the growth in world trade. This growth, boosted by the general lowering of tariff and other barriers to trade, allied to a strengthening of AML/CFT controls throughout the formal channels of transmission of funds, appears to have

had the effect of diverting an increasing flow of illicit funds into TBML. Indeed, FATF has expressed the concern that, as control is tightened in respect of other means of money laundering TBML is likely to become more attractive. The World Bank has estimated that some $1.5 trillion is paid in bribes to corrupt customs and related organisations and individuals each year.

Similarly, Europol in a report in 2015 stated that TBML was thought to have "significantly developed and increased" in recent decades due to the rapid globalisation of trade.

At the same time, the lower standards of AML/CFT control in some parts of the world, and the impact of bribery and corruption (which appears to particularly affect the movement of goods in certain regions), combine to contribute to the risks that TBML can exist and can go undetected.

In 2012, a global fraud survey conducted by Ernst & Young revealed that 90% of Foreign Corrupt Practices Act actions brought by the US Department of Justice involved misconduct by a company's third party.

In 2013, the Financial Conduct Authority (FCA) in the UK undertook a thematic review into UK banks' control of financial crime risks in trade finance. Following this, it warned banks that it expected them to implement appropriate systems and controls to prevent international trade finance from being exploited by organised crime and terrorist financiers to launder their ill-gotten gains. The FCA also included examples of goods and bad practice in a new chapter of its guidance ("Financial Crime: a Guide for Firms").

In January 2015, in a white paper published by PwC in the US, it was stated that the rise in TBML presented serious and costly risks associated with a growing number of fraudulent transactions. A research and advocacy organisation, Global Financial Integrity (GFI), estimated that as much as 80% of the illicit financial flows from developing countries were channelled using TBML methods.

Using trade data, GFI estimated in December 2014 that $950 billion flowed illicitly out of poor countries in 2011, excluding trade in services and fraudulent transfer pricing. 80% of this was by means of TBML linked to arms smuggling, drug trafficking, terrorism or public corruption. TBML is sometimes also referred to as a form of "trade-based financial crime".

In June 2016, the US Congressional Research Service published a report highlighting the importance of trade-based money laundering, its value and that one of the most common schemes involved over- or under-invoicing of goods and services. The report is available at - https://www.fas.org/sgp/crs/misc/R44541.pdf

In August 2016, a study by a professor at Florida International University College estimated the cost of false invoicing to the US authorities between 2003 and 2014 was more than $2.3 trillion. The analysis involved 12 years of US customs data and the author claimed that abnormally priced goods were used to mask complex tax avoidance schemes, and that the overall figure had grown by some 30% over the period - from $168.3 billion in 2003 to $230.6 billion in 2014, despite improved understanding of the threat and efforts to combat trade-based money laundering.

In an interview, the author of the study suggested that monitoring should concentrate on invoices, manifests, bills of lading and customs documentation - as a lie on a commercial invoice may be just a civil matter, but a falsehood on a customs document might be a criminal offence, and therefore the declarant might be more careful, and more truthful.

The study can be found at - https://business.fiu.edu/pdf/trade-based-tax-evasion-and-money-laundering.pdf

2. **What can trade-based money laundering involve?**

TBML can be achieved by -

a. misrepresenting the price, quality or quantity of goods being bought and sold, transported, imported, exported or otherwise traded; or

b. creating a partly or wholly bogus trading arrangement, or trading pattern, that can be used to justify the movement of value from one place or person to another.

The above can involve -

a. false invoicing (including misdescribing the type and quality of goods or services involved);

b. over-invoicing (overcharging);

c. under-invoicing (undercharging);

d. double-invoicing (and multiple billing, where two or more invoices purport to involve the same goods);

e. wholly fictitious transactions (where no goods or services are actually involved, a.k.a. "ghost shipping" or "phantom shipping" or "fictitious trades");

f. circular trading (as in carousel fraud, with the same goods being repeatedly "sold" to cover transfer of value as a result);

g. using counterfeit goods masquerading as genuine, and priced as if the genuine articles - and the trafficking of counterfeit goods would be, of course, criminal smuggling;

h. overstating or understating other costs (for transportation, for example, or storage, processing, packing etc); or

i. diversion of the goods from their original stated destination. Including back into their original country of origin (the latter also known as "U-Boat shipping").

Any one or more of these methods may be involved, and otherwise legitimate businesses could be used to transport or handle any goods involved. Alternatively, the whole transaction may be entirely false - with "paper" parties and all the necessary documentation also being counterfeit.

One should bear in mind that not just "goods" may be involved (whether real or fictitious). Real or fictitious services could just as easily be involved. Indeed, a complex laundering system may involve both real and purported movements of goods and real or imaginary "services" (such as consultant, inspection, insurance, etc).

The laundering may be the chief or sole aim of any activity, or it may be entirely incidental, allowing the criminal to seek to clean up the proceeds at the same time as carrying out his or her fraud.

The GFI advocacy group has identified four primary reasons for misinvoicing involving developing countries -

a. money laundering - criminals or public officials may seek to launder the proceeds from crime or corruption;

b. directly evading taxes and customs duties - by under-reporting the value of goods, importers are able to immediately evade substantial customs duties or other taxes;

c. claiming tax incentives - many countries offer generous tax incentives to domestic exporters selling their goods and services abroad. Criminals may seek to abuse these tax incentives by over-reporting their exports;

d. dodging capital or exchange controls - many developing countries have restrictions on the amount of capital that a person or business can bring in or out of their economies. Investors attempting to break these capital controls often misinvoice trade transactions as an illegal alternative to getting money in or out of the country.

Some, or all, of these may equally apply to developed countries.

Abuse of trade finance - TBML can also be taken to refer to misuse or fraud involving trade finance. Trade finance refers to where short-term financing is used to facilitate import and export activity, typically through various forms of letters of credit.

3. **Why is it important to be aware of the risk?**

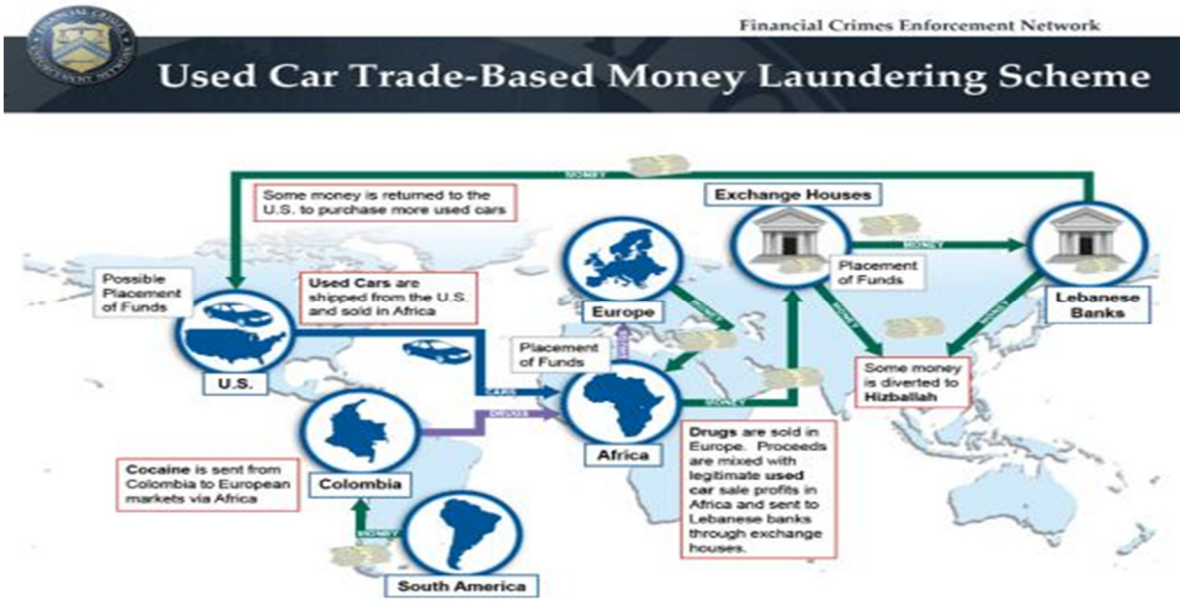
In the Isle of Man, TCSP, legal firms, banks and other financial institutions subject to AML/CFT control have an important role in combating TBML. If the awareness of TBML in these sectors is raised then this should reduce the Island's vulnerability to TBML risks.

The large and successful TCSP sector in the Island may mean that TBML is a potentially significant risk for the Island. What makes the sector attractive to legitimate business can also make it attractive to money launderers.

As well as any risk to the business or individuals concerned, the business sector and the Island as a whole could suffer serious reputational damage if it were thought that the Island was being used as a means to facilitate TBML.

4. **It is not just criminals that might use it**

The abuse of international trade is not limited to criminals and criminal organisations, and those avoiding or evading tax or exchange controls.



In 2014, the US authorities issued a $102 million forfeiture order to a Lebanese bank implicated in a scheme involving the export of used cars to West Africa with the proceeds funnelled to Hizballah.

In 2015, a leaked Turkish report highlighted alleged links between Turkish front companies, Iranian banks and money exchangers in Dubai whereby invoice values were inflated (e.g. $240 for a pound of sugar) to allow Iran access to hard currency for oil sales.

5. **How might it affect business in the Island?**

Whilst banks and other financial institutions, like their counterparts in other jurisdictions, may be affected, in the Island it is the number of TCSP which are involved in international trade that may present a particular risk.

A criminal or terrorist might see using an Isle of Man TCSP to form and/or manage one or more of the components in a TBML scheme as attractive. This can be because the Island would be far from where the actual or purported movements are taking place, probably in a distant time zone, and with all the obvious difficulties of verifying the identity of goods, shipments, documents etc. In addition, they may also be attracted by possible tax advantages, as well as the air of legitimacy the use of a British vehicle or address might convey.

6. **What indicators might there be that it is taking place?**

The same sorts of doubts and suspicions that may give cause for suspicions of other types of money laundering or unlawful activity can be a factor in respect of TBML.

Various organisations have highlighted a number of indicators, or "red flags", which may give rise to suspicions (see section 8 below).

In essence, the best defence is to ensure that your KYC and ongoing due diligence procedures are thorough and effective - remembering that one needs to be aware of all the parties involved in a transaction, whether the transaction is a viable, realistic commercial proposition, and that any checks on the transaction and the parties involved are satisfactory.

7. **What can I do to prevent or detect it?**

All those in the supply chain - exporters, importers, freight forwarders and carriers - as well as tax and customs authorities and law enforcement have a role to play. In addition, those that facilitate trade in other ways - such as a TCSP that helps to form and/or administer a trading company also have an important role.

In theory, all those involved in the supply chain (in its widest sense) should implement AML/ CFT preventive measures, including having a requirement to employ customer due diligence and KYC, have a suitable compliance officer and a reporting system for suspicions, as well as maintaining adequate internal records of checks and controls. A procedure for reporting any suspicions to the appropriate authority should be in place.

In Annex B is a checklist that those involved in a supply chain might find useful in undertaking due diligence checks.

To improve supply chain security your business could apply to become an Authorised Economic Operator (AEO) and only use third party suppliers and partners that are themselves AEO-certified. The AEO certification standards are designed to operate under the SAFE framework developed by the World Customs Organisation. The AEO programme may use other names in different countries, such as C-TPAT in the USA. AEO certification may also have other benefits, such as guarantee waivers and reduced customs compliance requirements.

In practice, whilst the move towards improving the security of the international supply chain - though chiefly for revenue and anti-terrorism purposes (such as by adoption of trusted traders or authorised economic operator programmes) go some way to help, it remains the case that of those businesses mentioned above many may not be subject to a formal AML/CFT control regime.

Unlike other specific areas of concern (such as for cash couriers), the current FATF Recommendations do not explicitly make direct mention of TBML. However, inherent in several of the Recommendations are the principles that, if applied, would tend to reduce the risk of TBML (e.g. a risk-based approach, KYC and due diligence procedures and so on).

Other Recommendations (such as Recommendation 32 on cash couriers) refer in passing to controls to be applied in trade situations. Annex I to the current FATF 40 Recommendations also includes mention of the FATF Best Practices Paper on Trade Based Money Laundering of June 2008 as relevant additional guidance.

TCSP administering a company should know what that business is doing. It is therefore probably somewhat easier for a TCSP to have a means of assessing the credibility and viability of their client's business.

However, it may be unreasonable for a TCSP to know the precise details of every transaction undertaken by clients and client companies. This may be particularly the case where the beneficial owner, or his or her family or close associates, conducts much or all the actual day to day running of the business. Thus it seems reasonable that where such responsibility is devolved to persons outside the direct control of the TCSP, that TCSP should attach a higher risk level (and additional in-house controls) in response.

In 2013, the FCA highlighted good practice in UK banks, such as -

- having clear roles and responsibilities for managing financial crime risks in trade finance;
- requiring staff to identify customers and transactions that represented the greatest risk;
- requiring staff to screen all relevant parties in a transaction;
- having detailed guidance available for staff on what might be potentially suspicious transactions (including lists of "red flags"); and
- encouraging processing teams to escalate any suspicions for investigation as soon as possible.

In addition, the FCA considered that having independent expertise from outside the trade finance business (e.g. the compliance department) involved in decisions and possible reporting of suspicions in SAR was best practice. Whilst a smaller TCSP may not have the separate sections that the FCA envisaged for UK banks, the principle of obtaining information, advice or assistance from as wide a spectrum as possible remains a good one.

The PwC white paper of January 2015 identified the use of "Big Data" techniques to data mine and analyse information. In the US, the Trade Transparency Units have been established to carry out such analysis of trade data, covering trade data in several Latin American countries, Australia and the Philippines. By sharing data, the US and foreign authorities are able to see both sides of an import/export transaction for commodities entering and leaving their countries.

The FATF best practice guidance on TBML in 2008 recommended improved compliance training for competent authorities (including for law enforcement), on the existence and usefulness of trade data and awareness-raising for those competent authorities and for business. It also recommended the setting up of Trade Transparency Units, like those found in the US.

In the US, FinCEN has used Geographic Targeting Orders (GTO) imposing lowered reporting thresholds and additional record-keeping requirements where the risk of TBML is considered to be high. In 2015, it issued a GTO affecting exporters in the Miami area citing the risk from Mexican drugs cartels. This followed GTO issued in respect of the fashion district of Los Angeles in 2014.

8. **What are the "red flags" that might alert one to it?**

In the US, ICE has identified several "red flags" that may indicate the existence of TBML -

- payments to a vendor by unrelated third parties;
- false reporting (such as misclassification of commodities, or under- or over-valuation);
- repeated importation and exportation of the same high-value goods (the carousel fraud mentioned above);
- commodities being traded that do not match the business or businesses involved;
- unusual shipping or transhipment routes;
- packaging which is inconsistent with the commodity or shipping method (e.g. goods that require specialised transportation, such as refrigeration, lacking such requirements); and
- double-invoicing.

In the UK, the FCA suggested the following matters, (which can be seen to have general application and not just limited to banks providing trade finance) may be indicators.

Transactions which -

- lack business sense or commercial strategy;
- are inconsistent with the customer's stated business strategy;
- deviate from the normal pattern of trading;
- involve parties sharing the same address, or provide only a registered agent's address;
- involve excessive or aggressive pressure from the client;
- involve an apparent reluctance to provide clear answers to routine questions;
- use structures that appear unnecessarily complex and/or designed to obscure the true nature of a transaction;
- have an unusual number of intermediaries;
- involve one or more of the parties being a shell company;

- involve unexplained changes to payment instructions;
- include requests to pay a third party;
- involve the use of cash;
- involve unusually favourable payment terms, or has an unusual trigger point for payment; or
- does not make economic sense (e.g. the container is too large).

Documents -

- where shipment locations, shipping terms or descriptions of goods are inconsistent (for example, when compared to any Letter of Credit);
- with significant discrepancies between descriptions of the goods on bills of lading or airwaybills and the actual goods said to have been shipped;
- with unauthorised amendments to documents;
- where Bills of Lading are consigned "to be advised between applicant and beneficiary" or the like;
- including future-dated Bills of Lading; or
- where the Letter of Credit etc contains non-standard clauses.

Research carried out by Dutch police noted the use of cash being a significant factor which characterised TBML schemes. A number of cases showed goods being paid for in cash, in one example the buyer paid with no less than 3,750 €20 banknotes. Normally cash payments would only constitute a small proportion of the expenditure of companies, and such large cash transactions should automatically trigger suspicions.

9. Case studies

There follow a number of cases involving TBML.

(a) One case study that can be considered is very close to home. In 2002 it was reported that, following an investigation instigated by Customs and Excise under the Island's AML laws, and latterly in partnership with authorities in the US, UK and Colombia, arrests were made in Colombia, and some $8.75m was seized.

A complex scheme to launder the proceeds of Colombian drugs traffickers using the international life insurance industry was found to involve the Island. This employed a system of brokers, policies and the so-called "Black Market Peso Network".

In February 2016, the DEA stated that Hezbollah continued to launder significant sums, the proceeds of drug trafficking, using the Black Market Peso Exchange, having established connections with South American cartels. The US Treasury added two Lebanese businessmen to its sanctions listings, citing their involvement in such laundering.

(b) Also as long ago as 2002, the International Chamber of Commerce (ICC) highlighted a case where a fraudulent seller sold a cargo of over 70,000 tons of crude oil located in a tank farm in Kazakhstan. The buyer opened a letter of credit which called for a bill of lading to be presented to the buyer's bank confirming that the cargo had been

consigned. The seller then procured a bill of lading and other documents which purported to show that the oil was awaiting shipment by pipeline to Latvia, for eventual onward shipment to Finland. These documents were presented to the bank which then paid out under the letter of credit. The oil itself never existed, and the NVOCC (shipper) which issued the fraudulent bill of lading turned out to be a hollow shell. According to the ICC, it was arguable that an experienced banker with a knowledge of shipping would have found the circumstances involved highly irregular. This case is said to highlight the need to ensure that shippers and others that are used are "substantial", signalling the need for adequate due diligence to be undertaken on all relevant parties in a supply chain.

(c) Authorities in US had information that a bank in Lebanon had been extensively used by an international drug trafficking syndicate controlled by an individual for moving the proceeds of narcotics sales through TBML across the globe.

The syndicate smuggled narcotics from South America to Europe and to the Middle East through West Africa. The kingpin of the syndicate organised shipments of 100 tonnes of cocaine from South America and laundered the proceeds of up to $200m per month, obtained from the sale of cocaine in Europe and the Middle East.

The proceeds were moved and laundered through bulk cash smuggling (cash couriers), the use of exchange houses (including one owned by the kingpin), and the use of accounts of family members in several branches of the bank.

Bulk cash deposits were made by the kingpin and his associates into exchange houses which in turn deposited the money into several accounts maintained in the bank. In fact, he owned and controlled one of the exchange houses located in the same building as a branch of the bank, and some employees of the bank were also involved.

(d) US Customs investigators uncovered a scheme employing the Black Market Peso Network in which a Colombian cartel used proceeds from drug sales to buy stuffed animals in Los Angeles, exporting them to Colombia. Sales of the toys in Colombia enabled the cartel to bring its ill-gotten gains home, convert them to pesos and get them into the banking system.

(e) A Global Financial Integrity report in December 2014 highlighted the following examples:

- the under-invoicing of imports, particularly of construction materials, by Philippine firms evading customs import duties and VAT meant that an estimated 25% of that country's imports did not appear in national statistics;

- India's official exports to the Bahamas rose a thousand-fold between 2008 and 2011, probably because of a surge in over-invoicing by Indians taking home money held in undeclared accounts, before a tax-transparency agreement between the countries came into force; and

- Chinese firms and individuals sought to evade capital controls and repatriate money parked in Hong Kong, causing exports from the Chinese mainland to Hong Kong to be over-reported by $101m in 2012 - nearly as much as total foreign direct investment into China that year.

(f) One group of Czech money launderers was reported as having exported plastic buckets to the USA, invoicing them at a price of $970 each.

(g) A company in India received an advanced remittance from a company in another country for an export consignment of diamonds. The Indian company then filed false

declarations (and forged documents) to over-value the diamonds and to show that exports had taken place (when, in fact, none had). It also fabricated purchase invoices to "prove" that it had bought the diamonds in. It also claimed export finance payments from the Indian authorities.

In fact, the Indian company had also been operating a high-yield investment (Ponzi) scheme, and had transferred the funds raised to the foreign company involved using the *hawala* informal remittance system - receiving back into India the funds as "payment" for the diamonds that had ostensibly been exported.

Consequently, the proceeds of the crime in India had been cycled through another country and flowed back to the criminals by means of a TBML arrangement.

(h) Criminal groups physically transported €500,000 to €900,000 in cash per week from Western to Eastern Europe, the cash being generated by criminal activities, including the import and sale of counterfeit or sub-standard consumer goods from Asia, sold at greatly reduced prices. The cash was deposited in the accounts of "trading companies" in Eastern Europe (with one of the cash couriers having connections to the commercial bank involved). The cash was then transferred to accounts in Asia, also allegedly held by trading companies, masquerading as relating to international trade deals and payment for goods. It was estimated that no less than €100m and $300m was laundered using just 5 bank accounts in this case; but with at least 60 additional companies being identified.

(i) Fence posts from Vietnam are shipped to France, with only half their true wholesale value being quoted. The invoices and shipping documents all mispresented the actual value or the amounts of goods shipped. As a result, both the exporter and the importer saved on taxes, and on import and export duties.

(j) In 2014, a Chinese trading company used forged warehouse receipts to borrow multiple times against non-existent metals allegedly stored in a warehouse, thus using it as collateral for loans or as a cheaper form of financing for other purposes. In this case, repeatedly using warehouse receipts to borrow against the same asset amounts to fraud. This case raised the question of what checks should the banks involved have done to substantiate the trade documents and the underlying trade.

This last case well illustrates several of the "red flags" that, if detected, can arouse suspicions of TBML - the export of goods without any corresponding purchases of either the goods or the raw materials to produce them; a sudden increase in volume of trade by a new exporter; a substantial advance payment against exports without a justifiable reason; and exportation documentation that was not properly authenticated by the relevant authorities (but which were accepted by the banks concerned).

(k) In November 2015, 16 members of a Midlands-based money laundering network were jailed for a total of 74 years for their part in laundering over £35 million through UK banks and money service businesses. A number of bogus clothing and textile companies were set up to provide a mechanism for the apparent purchase of goods, which then justified the flow of funds. False invoices were produced, bank and trading accounts used, but no trading actually took place. If any bank or MSB raised concerns about any of the companies, it would be closed down and a new one set up. An accountant was one of the gang, and had advised the leader how to operate without alerting HMRC or law enforcement. The leader of the gang, Harpal Singh Gill, a former textile trader, received a sentence of 11 years.

(l) In late 2015 it was reported that substantial frauds involving fraudulent use of bills of exchange had resulted in very large losses at two Chinese banks. In one case, a bill of exchange was illegally sold by bank employees to a third party, who then in turn sold it

to another bank. The bank employees used the funds they obtained to speculate on the stock market, suffered losses and were unable to pay the money back. Another fraud also involved the fraudulent obtaining of funds to invest in the stock market - but in that case an established financing agent cashed bills of exchange for his own use. The China Banking Regulatory Commission highlighted what it described as "imprudent behaviour" in trade finance in a notice issued in December 2015.

(m) In 2016, reports from India highlighted the use of patent owners who sold their intellectual property in front of companies overseas, in schemes that enabled money to enter or re-enter the domestic economy, ostensibly as the legal earnings from the IP involved. An example given was where an Indian company formed a partnership with the holder of a patent, with the patent then "sold" to a business outside the country, with the payment for the sale being received as legitimate funds. In many cases, the funds involved were said to have originated in India, as the proceeds of tax evasion, for example, and sent abroad using informal means (such as hawala). The IP owner and the overseas company receive a share of the proceeds as a form of "commission". In India, providing such cover for the funds involved reduced the potential tax charge from 30% or 45% to 10%, whilst seeming to involve a legitimate and successful business operation.

(n) In July 2016 the use of clothing and footwear imports into Colombia by the Mexican Sinaloa drug cartel was reported in a trade-based money laundering case. This exploited a loophole in Colombian law where such imports were exempt from import duties where the goods originated from a country with a free trade agreement with Colombia. The criminals merely falsified the countries of origin, thus avoiding import duties whilst laundering their money. The products were funnelled through the fashion district of Los Angeles (which resulted in the Geographic Targeting Orders imposed in the US on businesses in the district). The case came to the notice of the authorities when they noticed the rapid and unusual increase in the amounts of clothing and footwear being imported from countries that had not previously been large exporters of such goods.

(o) In 2012, Colombia adopted a compound tariff on imports of certain textiles from Panama which came into effect in 2013, contending that GATT (now WTO) international trade rules did not apply to illicit trade, and even if the tariff was inconsistent with the rules it was justified as a measure to protect "public morals" and ensure compliance with Colombia's laws combating money laundering.

This drastic measure to counter suspected trade-based money laundering was challenged at the WTO by Panama.

Colombia claimed the goods involved were commonly imported at artificial low values to enable the laundering of money. However, in 2016 the WTO ruled that the initiative did breach its rules, in that it did not distinguish between legitimate and illicit trade. In November 2016, Colombia passed new laws to remove the compound tariff.

The WTO Panel report can be found at -
https://www.wto.org/english/tratop_e/dispu_e/461r_e.pdf

9A. **Transaction laundering**

This is the term describing situations where legitimate merchants set up a scheme to process payments (usually involving credit or debit cards) for illegal goods on behalf of another merchant (aka merchant account laundering, factoring or undisclosed aggregation). A merchant sets up an online store and receives approval of a bank or payments provider to

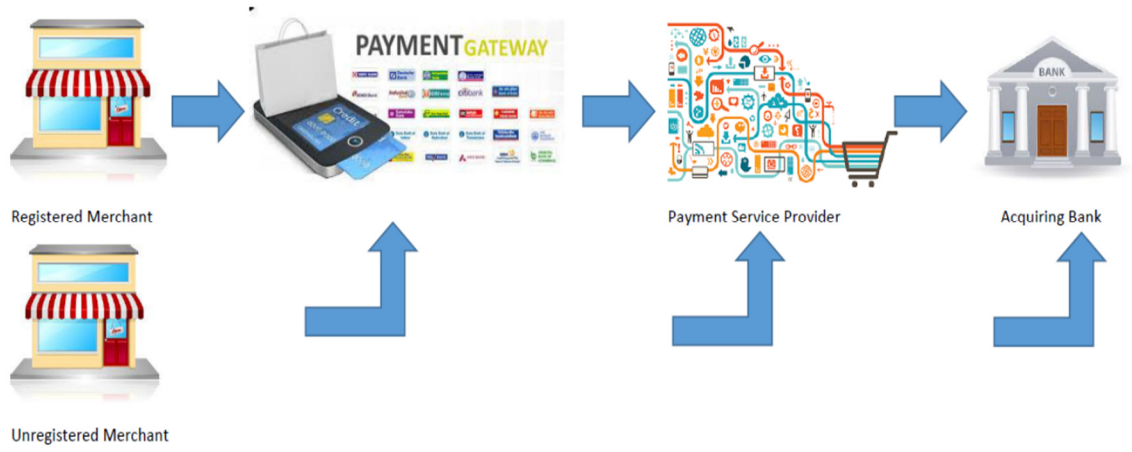
process orders, he or she then sets up additional websites to sell other, illegal goods with payments being routed via the legitimate online store.

In 2017, in the USA it was estimated that perhaps $6 billion was involved in transaction laundering and illegal goods, sold online by nearly 35,000 unregistered merchants.

An example in 2016 involved a specialty pharmacy in New York that provided medications and support services to HIV patients, but was also found to be providing expired or counterfeit HIV medications. The case involved a complex arrangement of different persons and sites, and shell companies, with fabricated sales, routing purported sales through the shell companies, and even physical repackaging of the medications.

The original specialty pharmacy was itself legitimate, and was used because it was an ideal and inconspicuous (and seemingly worthy) front for the other, illicit transactions.

In August 2017, the FBI reported that a US citizen had used transaction laundering in fraudulent sales of computer printers over eBay, receiving nearly $10,000 for support of ISIS through overseas sales through PayPal. The FBI suggested that this was not an isolated case.



10. What do I do if I have suspicions?

As with any suspicion of money laundering in general, you should follow your internal reporting procedures.

If need be, you should make every reasonable effort to verify independently the transaction or party that is giving rise to the suspicion. You should, of course, have undertaken the normal KYC and ongoing due diligence procedures for your client and their activities. These could be reviewed and/or repeated, again using alternative or independent sources, if possible.

If suspicions remain, a SAR should be made to the FIU.

You may also need to report any suspicions to the Customs and Excise Division. If any part of the suspected criminal activity involves -

- the movement of goods between countries;
- importation into or exportation from the Isle of Man/UK or EU;
- the import into the Island of any prohibited or restricted goods (e.g. illegal drugs and the precursor chemicals to make them, firearms, endangered species);

- the evasion of customs or excise duties or VAT, or the avoiding or evasion of customs controls;
- the movement of large sums of cash to or from the Island or the UK;
- any matter to which UN or EU financial or trade sanctions controls may apply;
- the movement of certain controlled goods between other countries (where a trade control licence may be required in the Island - see Notice 279T MAN),

you should contact Customs and Excise.

11. **Where can I get more information?**

On TBML -

- FATF Best Practices Paper on Trade Based Money Laundering (June 2008)
- FATF Asia/Pacific Group (APG) Typologies Report on Trade-Based Money Laundering
- AUSTRAC typologies and case studies report 2014
- Illicit Financial Flows from Developing Countries 2002-2006 (Global Financial Integrity, December 2014)
- Wolfsberg Group[1]
  - issued guidance in 2006 on using a risk-based approach for managing money laundering risks[2];
  - in 2015 issued frequently asked questions on risk assessments for money laundering, sanctions and bribery & corruption[3]; and
  - in 2017, together with the Banking Commission of the International Chamber of Commerce (ICC) and BAFT (an association for organizations actively engaged in international transaction banking), issued Trade Finance Principles which dealt with money laundering, as well as UN and EU sanctions and proliferation issues[4].
- In September 2017 the US Bankers Association for Finance and Trade (BAFT) issued "Combatting Trade Based Money Laundering - Rethinking the Approach"[5].
- A new FATF-Egmont Group report aims to help public and private sector with the challenges of detecting trade-based money laundering
  FATF/Egmont Trade-based Money Laundering: Trends and Developments

1 Wolfsberg Group is a non-governmental association of global banks, founded in 2000; http://www.wolfsberg-principles.com/index.html
2 http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_RBA_Guidance_(2006).pdf
3 http://www.wolfsberg-principles.com/pdf/faq/Wolfsberg-Risk-Assessment-FAQs-2015.pdf
4 http://www.wolfsberg-principles.com/pdf/standards/Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf
5 http://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paperf246352b106c61f39d43ff00000fe539.pdf?sfvrsn=2

On other related matters -

- Trade control licensing
- Export licensing controls, including cultural items
- UN and EU sanctions

See the Customs and Excise webpage on Sanctions and Export Control

Privacy Notice

The Treasury collects information about you in order to administer taxation and carry out other functions for which it is responsible (e.g. National Insurance, customs and excise duties, property rates, social security benefits, state pensions and legal aid etc.), and for the detection and prevention of crime.
Whilst that information will primarily be provided by you, where the law allows we may also get information about you from other organisations, or give information about you to them. This may be to check the accuracy of the information provided, prevent or detect crime or protect public funds in other ways. These organisations may include other government departments, the police and other agencies.

To find out more about how we collect and use personal information, contact any of our offices or visit our website at: https://www.gov.im/about-the-government/departments/the-treasury/privacy-notice/

Annex A

FATF Recommended Techniques for the Analysis of Trade Data

a. Comparing domestic and foreign import/export data to detect discrepancies in the description, country of origin, manufacturer, importer/exporter, ultimate consignee, broker, unit price, commodity activity by time period, and port of import/export.

b. Analysing financial information collected by the FIU to identify patterns of activity involving the importation/exportation of currency, deposits of currency in financial institutions, reports of suspicious financial activities, and the identity of parties to these transactions.

c. Examining cargo movements through the comparison of import/export documentation between two countries to verify that the data reported to one country's authorities matches the data reported to the other country's authorities.

d. Examining domestic import data with an automated technique, such as Unit Price Analysis, to compare the average unit price for a particular commodity and identify traders who are importing commodities at a substantially higher or lower price than the world market.

e. Comparing information such as the origin, description and value of the goods, particulars of the consignee and consignor, and the route of shipment with intelligence information in existing databases to detect any irregularities, targets or risk indicators.

f. Using statistical analysis methods, such as linear regression models, on trade data concerning individual, non-aggregated imports and exports.

g. Comparing export information with tax declarations to detect discrepancies.

h. Paying particular attention to trade transactions that display known red flag indicators of TBML/FT activity.

i. Cross-comparing known typologies of risk (such as those identified in the FATF Typologies Report on Trade-based Money Laundering) with trade data, information on cross-border monetary transfers associated with the payment of goods, intelligence, tax and wealth information.

j. Taking appropriate follow-up action when anomalies and discrepancies in trade and financial transactions are identified. Depending on the circumstances, appropriate follow-up action could involve asking the trader for further explanation and supporting documents; auditing traders who have presented discrepancies to check the volume of their business, regularity of their operations, the kinds of goods exported, and connections with organised crime or any other illicit activity; and/or making the completed analysis available to the investigative authorities.

In addition, in order to facilitate international co-operation in combating TBML/FT, countries could establish clear and effective gateways, subject to appropriate controls and safeguards and existing legal frameworks, to facilitate the prompt and effective exchange of trade data and other relevant information, on a case-by-case basis or as otherwise appropriate, with authorised counterparts in other jurisdictions, by means of both informal and mutual administrative arrangements, and through formal mutual legal assistance.

FATF also concluded by saying that the following steps could be taken without undue adverse effect on legitimate trading activity -

a. applying an intelligence, risk-based and target-based approach which makes consistent use of TBML/FT red flag indicators;

b. using data capture mechanisms such as Electronic Data Interchange (EDI), which is a set of standards for standardising the structure of information to be electronically exchanged between authorities, from one computer system to another, without human intervention and subject to appropriate data protection safeguards;

c. authorising traders that meet certain criteria to benefit from facilitations for customs controls or simplifications for customs rules (e.g. in the EU, Authorised Economic Operator (AEO) status may be granted to traders that meet the following criteria - an appropriate record of customs compliance, satisfactory management systems that allow appropriate customs controls, adequate security and safety standards, and proven solvency);

d. utilising the trade data that is gathered automatically from customs declaration forms thereby avoiding any extra burden for the traders who are involved in legitimate trade;

e. conducting non-intrusive inspections of goods being imported and exported using scanners;

f. having authorised domestic authorities (e.g. customs, FIU) share information either upon specific request or spontaneously;

g. providing information to foreign authorities and placing conditions on the use of such information;

h. establishing a Trade Transparency Unit to facilitate the sharing and analysis of import/export data. Because the system does not rely on real-time trade information to target data (the system uses historic data to identify anomalies that are indicative of TBML/FT), legitimate trading activities are not unreasonably hindered.

Annex B

Suggested checklist where movements of goods are involved

As part of a risk-based approach, the following checklist might be considered as a starting point for undertaking due diligence. It cannot be comprehensive, and could be adapted to suit the circumstances of the particular trade or business involvement.

Is the transaction -

- Credible? - does it make sense, what is the rationale or justification?
- Viable? - does it make commercial sense? Is the unit price realistic? Have you/can you verify the approximate valuation from publicly available sources?
- Evidenced?

Are all the parties identified, and have you carried out reasonable due diligence - seller, buyer, end-user, shipper(s) do they have substance or even exist?

Are there any discrepancies in or between supporting or associated documentation (e.g. letters of credit, invoices, bills of lading or airwaybills), or have there been any unauthorised or unusual alterations or amendments?

Have you carried out checks against sanctions lists (IOM/UK, EU, US) or other reference sources?

Is the destination -

- Credible? - does it make sense to send such goods to that place, or to use the intended routing?
- High-risk? - for corruption, diversion, conflict zone
- Vulnerable to diversion? - to other undeclared destinations or users
- Close to sanctioned or embargoed countries?

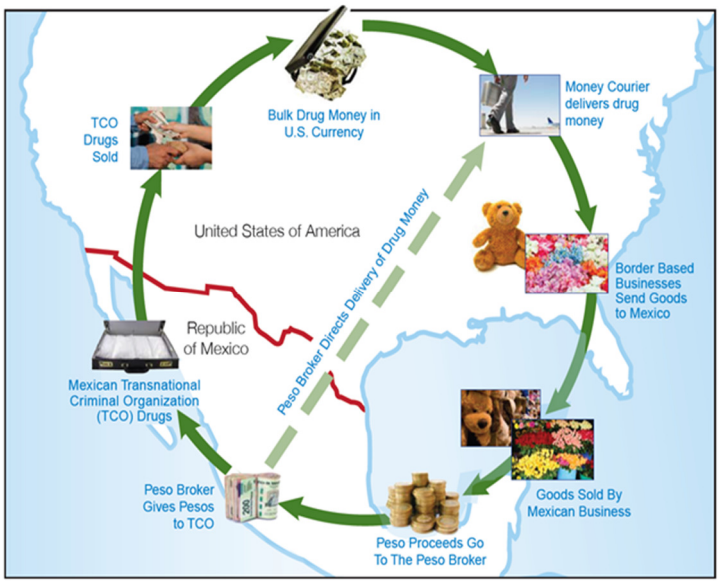
Are the goods -

- High risk? - goods vulnerable to trade-based money laundering are said to include precious metals and gems, jewellery, cigarettes and tobacco products, mobile telephones and other high-value consumer electronics, telephone and stored-value cards
- Adequately identified and described?
- Military or paramilitary?
- Law enforcement items, or capable of use in repression?
- High-tech (including surveillance or encryption devices and software)?
- Dual-use - with both a legitimate civil and potential military use, or in the development or use of WMD, including missiles, chemicals etc

- Subject to licensing by the UK, EU, US?

- Covered by trade control licensing (where goods moving between two third countries without touching the Isle of Man, or UK?) - see Notice 279T MAN.

Glossary

AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
Bill of Exchange	An unconditional order in writing requiring the person to whom it is addressed to pay on demand, or at a fixed or determined future time, a sum of money to, or on order of, a specified person or to the bearer. They are short-term debt instruments commonly used in international trade. As with other forms of debt instrument, they may be sold at a discount to another person before payment is due.
Black Market Peso Network (or BMPE)	This term is used to describe the means by which drugs money is moved from the US to the source country. It operates through brokers who purchase narcotics proceeds in the US from the cartels and transfer funds to the cartels from within the source country (e.g. Colombia). The dollars are placed ("laundered") into the US financial system by the broker without attracting attention (perhaps by means of a "funnel account". The dollars are then "sold" by the brokers to businessmen in Colombia who need dollars to buy US goods for export. Goods ready for export are often actually paid for by the peso broker, using the purchased narcotics dollars, on behalf of the Colombian importer. BMPE-like methodologies are also found in Asia, Africa and elsewhere.  https://oag.ca.gov
FATF	Financial Action Task Force

FinCEN	Financial Crimes Enforcement Network (US Treasury)
FCA	Financial Conduct Authority
FT	Financing of terrorism
Funnel accounts	In the US, restrictions under AML law in the US and Mexico there led to the use of "funnel accounts" where a person or business receives multiple cash deposits (usually below the reporting threshold), with the funds then being withdrawn somewhere else (e.g. received in Boston and withdrawn in the border area in or with Mexico), with only a short time elapsing between deposit and withdrawal. Goods are bought with the withdrawn funds by a Mexican business and sold in Mexico for pesos - meaning that the drug cartel has exchanged dollars for Pesos, whilst providing an apparently legitimate cover for the proceeds of drug trafficking in the US. The US or Mexican business or businesses involved can be genuine, otherwise legitimate businesses, with their involvement in the drugs trade limited to their facilitating the movement and exchange of the proceeds.
Hawala	A broker system based on trust, found throughout South Asia, the Arab world and parts of Africa, and in Europe and the Americas. It allows customers and the brokers to transfer money or value without physically moving anything - and is often used in areas where there are few or no banks and other financial institutions available. "Hawala" is a catch-all term for a system known by different names (Hawala itself is an Arab term).
KYC	Know Your Customer
NGO	Non-Governmental Organisation
Phantom shipping	A term used to describe the use (or re-use of counterfeit bills of lading and other shipping documentation to provide cover for a consignment of goods which never existed. It may be used to avoid currency controls, integrate illicit funds in a money laundering scheme, defraud the importer or their bank, or to access relatively inexpensive funding to use for other, non-trade related, purposes.
SAR	Suspicious Activity Report
TBML	Trade-Based Money Laundering
TCSP	Trust and Corporate Service Providers

Transaction laundering (TL)	A form of online fraud where legitimate merchants process payments (usually involving credit or debit cards) on behalf of another merchant. Using TL, a merchant sets up an online store and receives the approval of a bank or payments provider to process orders, he or she then sets up additional, unregistered websites to sell other, illegal goods with payments being routed via the legitimate online store.
U-Boat shipping	The diversion of the goods from their original, stated destination back into the country of origin to avoid taxes or duties, for sale on the black market or insertion into the legitimate supply chain.

Amendments to this Notice

25 November 2015	New paragraph 9(k) inserted re further case study involving Midlands-based laundering gang (NCA news release, 24 November 2015).
2 February 2016	Addition to case study in paragraph 9(a), and new sub-paragraph (l) added to paragraph 9. Definition of a bill of exchange added to the Glossary.
2 March 2016	New case study added as paragraph 9(m), and data protection notice updated. Paragraphs 2 and 7 amended, and situations where Customs and Excise should be notified in paragraph 10 revised. New Annex B inserted.
1 August 2016	Paragraph 1 amended, and new paragraph 9(n) added, re use of TBML by Sinoloa drug cartel.
9 August 2016	Paragraph 1 amended to mention US study by John S. Zdanowicz PH.D., Professor of Finance, Chapman Graduate School of Business, Florida International University, Miami.
29 September 2016	Text and Glossary amended to make specific reference to U-Boat shipping and similar diversion frauds used in, or as part of, TBML.
9 February 2017	New paragraph 9A inserted, and definition added to the Glossary, concerned with transaction laundering.
14 February 2017	New sub-paragraph (o) added to paragraph 9 re the dispute at the WTO between Colombia and Panama over an additional import tariff imposed to counter allegedly undervalued imports from Panama for use in money laundering.
3 March 2017	In paragraph 11, information available from the Wolfsberg Group added.
6 March 2017	Definition of BMPE amended, and one for hawala added; paragraph 7 re TTU updated and amended.
24 May 2017	Paragraph 1 amended to mention DoJ FCPA statistics, and paragraph 7 amended to mention the use of AEO programmes.
29 September 2017	Paragraph 9A on transaction laundering expanded and diagram added.
6 July 2018	Privacy Notice added
10 March 2021	Link to FATF/Egmont Trade-based Money Laundering: Trends and Developments added

Published by:
Isle of Man Customs & Excise Division
PO Box 6
Custom House
North Quay
Douglas
Isle of Man
IM99 1AG

Telephone: (01624) 648100

Email: customs@gov.im
Website: www.gov.im/customs

This document can be provided in large print or audio tape on request

Isle of Man
Government
Reiltys Ellan Vannin