ICLG

The International Comparative Legal Guide to:

Anti-Money Laundering 2018

1st Edition

A practical cross-border insight into anti-money laundering law

Published by Global Legal Group with contributions from:

Allen & Overy LLP
ANAGNOSTOPOULOS
ASAS LAW
Barnea
BONIFASSI Avocats
C6 an Acuris Company
Castillo Laman Tan Pantaleon & San Jose Law Offices
Chambers of Anuradha Lall
Debevoise & Plimpton
DQ Advocates Limited
Drew & Napier LLC
DSM Avocats à la Cour
Duff & Phelps, LLC
Durrieu Abogados S.C.
EB LEGAL
Encompass
Gibson, Dunn & Crutcher LLP
Hamdan AlShamsi Lawyers & Legal Consultants
Herbert Smith Freehills Germany LLP
JMiles & Co.
Joyce Roysen Advogados
Kellerhals Carrard Zürich KlG
King & Wood Mallesons
Linklaters
Morais Leitão, Galvão Teles, Soares da Silva & Associados, SP, RL.
Navigant Consulting
Rato, Ling, Lei & Cortés – Advogados
Rustam Kurmaev & Partners
Shri Singh
WilmerHale
Yamashita, Tsuge and Nimura Law Office

glg
global legal group

global legal group

Contributing Editors
Joel M. Cohen and Stephanie Brooker, Gibson, Dunn & Crutcher LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Senior Editors
Suzie Levy
Caroline Collingwood

CEO
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2018

ISBN 978-1-912509-12-6
ISSN 2515-4192

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Through a Mirror, Darkly: AML Risk in Trade Finance

Alma Angotti

Robert Dedman

Navigant Consulting

Introduction

International trade is the lifeblood of the world economy. However, financing – or passing through funds from – international trade transactions places financial institutions at significant risk of being used as conduits for a variety of financial crime, including trade based money laundering (TBML), terrorist financing and certain forms of predicate criminality. And the financial value of such illicit flows of funds is potentially significant: Global Financial Integrity (GFI) estimated in a report published in April 2017[1] that in developing and emerging economies illicit inflows and outflows accounted for between 14 and 24% of their total trade in the years between 2005 and 2014. To give an idea of scale, the GFI report estimates that, in dollar terms, illicit inflows and outflows accounted for between US$620bn and US$970bn in 2014 alone.

Criminals exploit a number of factors to make use of the trade finance process for their illicit activities, including:

- the fact that the importer and exporter may be geographically distant from one another, and the importer may not even see the goods until they arrive at their port of destination;
- the fact that the underlying goods for which trade finance may traverse significant distances – most often by ship – and cross multiple borders; and
- the sheer volume of international trade makes it relatively straightforward to hide illicit transactions in plain sight.

While regulators and international standard setting bodies have – for more than a decade – published information for firms about how to identify and prevent TBML, regulatory action against financial institutions for TBML failings has been relatively rare. Despite the scarcity of significant enforcement action, regulators have set clear expectations of the industry, and when they have focused on the industry's approach to trade finance, they have found significant shortcomings in how financial institutions deal with TBML risk. As such, a strong compliance programme which aims to detect and prevent potential TBML is vital for any firm engaged in trade finance activity.

The different types of trade finance transaction also pose different levels of risk to financial institutions, and bring with them different challenges in terms of institutions' ability to detect illicit activity.

Documentary trade finance transactions[2] (which account for approximately 20% of all transactions) involve a bank issuing documents on behalf of a customer guaranteeing payment if certain specified terms are met[3]. Once the payment has been made, the goods are then released to the buyer. The financial institution concerned would therefore usually have access to the key documents evidencing the transaction, including a description of the goods themselves, details of their origin and destination (and sometimes the vessel on which they have been shipped), and the price paid.

However, the vast majority of trade finance transactions (around 80%) are carried out on an open account basis. Open account transactions generally occur where a supplier ships goods to the buyer who then pays for the goods within a period after receipt (which can be on a monthly basis for regular shipments, or as much as 90 days after receipt). They therefore pose considerable challenges for financial institutions seeking to identify TBML, because in a typical open account transaction unless some extra information is included in any associated SWIFT message, there will be limited (if any) information available to the institution over and above the identities of the parties to the payment and the amount to be paid.

In addition to money laundering and other forms of criminality, financial institutions engaged in trade finance must be alert to the possibility that the trade finance they provide could be used as part of a transaction, or series of transactions, designed to evade export controls, to finance nuclear proliferation or to finance terrorism. While this article deals only with TBML, it is clearly vital that firms have systems and controls designed to detect when a transaction involves those additional risks.

Trade Finance and Predicate Criminality

In addition to being a source of significant money laundering and terrorist financing risk for financial institutions, it is worth noting that the same features of trade finance that make it attractive to money launderers also mean that trade finance may be used for a variety of forms of predicate criminality.

Example 1 – Fraud

The paper-based nature of trade finance, and the fact that the underlying trade transactions cross borders makes it an obvious conduit for fraud. Fraud in trade finance transactions may take a variety of forms, including:

- shipping smaller quantities of goods than have been paid for, or goods of a lesser quality; and
- goods have been delivered, but no payment is made.

The difference between fraud in trade finance transactions and trade based money laundering can be found in the fact that trade based money laundering often results from collusion between two parties to a trade finance transaction, whereas fraud is committed by one party to the transaction without the knowledge of the other.

However, the red flags for a fraudulent trade finance transaction can be similar to those for TBML and it may only be as a result of subsequent investigation that a firm is able to categorise a potentially suspicious transaction as one or the other.

Example 2 – Bribery

The payment of a bribe can also be hidden in plain sight through an international trade transaction, and there are various ways that value may be transferred, depending on which way the bribe payment is intended to flow including:

- Under-invoicing – where goods with a greater value are invoiced at a lower rate. This will result in a transfer of value to the purchaser of the goods.
- Over-invoicing – where goods of a lesser value are invoiced at a greater rate, resulting in a transfer of value to the seller.
- Third party payments – where payment is made to, or by, an ostensibly completely unconnected third party.

While customer due diligence measures put in place by firms should detect the direct presence of Politically Exposed Persons (or other high risk individuals) in the transaction, often transactions involving high risk individuals will take place through shell companies of which the person concerned is the ultimate beneficial owner. As such, carrying out appropriate due diligence, and looking for inconsistencies within the transaction itself, will be key in terms of preventing trade transactions being used for bribery.

Regulatory and Law Enforcement Interest in Trade Based Money Laundering

Many regulatory and industry bodies offer practical guidance as to how firms can improve their detection of trade based money laundering, further insight of emerging trends and patterns as well as setting their expectation of the controls firms should already have in place as part of their compliance framework. For UK firms, key guidance has been issued by:

- **The Wolfsberg Group**, which published its updated Trade Finance Principles in January 2017[4].

  The updated principles cover all areas of TBML compliance, including Customer Due Diligence, name screening, financial sanctions, export controls, and the three lines of defence model. It also helpfully includes annexes giving a list of risk indicators and possible controls for different types of trade finance transaction (documentary credits, bills for collection, and standby letters of credit).

  In March 2018, the Wolfsberg Group also released an awareness video on TBML[5]. In doing so, the Group noted that: "Successful mitigation of TBML requires greater collaboration and information sharing between those other key international trade players in the public and private sectors. These include shippers, airlines, truckers, port and customs authorities, businesses and law enforcement agencies."
- **The UK Financial Conduct Authority (FCA)** in 2013, following a thematic review of UK banks' trade finance controls[6].

  The FCA's review noted that TBML controls at banks were generally weak, making key findings relating to: inconsistent approaches to risk assessment; an overall lack of policies and procedures; weaknesses in transaction monitoring and in identifying potentially suspicious transactions for further investigation; a lack of management information; and a scarcity of trade finance-specific training.

  The overall conclusion of the review was that the majority of banks sampled were not taking adequate measures to mitigate the risk of money laundering and terrorist financing in their trade finance business. The annex to the FCA's thematic review provides a number examples of good and poor practice, together with examples of potential red flags as they relate to customers, documents, transactions, shipments and payments.
- **The UK Joint Money Laundering Steering Group (JMLSG[7])**, which issues guidance to UK firms, has issued sector specific guidance relating to trade finance in Chapter 15 of Part 2.

  The JMLSG Guidance on trade finance brings together an explanation of trade finance and how it operates, alongside key compliance activities which Banks should undertake. It explains the difference between different types of trade finance activity, and how they may drive different approaches to matters such as customer due diligence, transaction monitoring and sanctions screening.
- **The Financial Action Task Force (FATF),** which published a detailed study in 2006[8], including a number of case studies of different types of TBML.

  The FATF study focusses on the importance of creating awareness and having strong training programmes to enhance the firm's ability to identify trade based money laundering techniques. It also suggests that firms should be using financial and trade data analysis to identify any anomalies within their data.

  In 2012[9], FATF's Asia Pacific Group produced a further study which set out in more detail a range of potential typologies for TBML, and associated red flags.
- **Bankers Association for Finance and Trade (BAFT)**, which published its guidance on *Combatting Trade Based Money Laundering – Rethinking the Approach in August 2017*[10].

  BAFT focus on alternative approaches to solving the problem of TBML and highlight the misconceptions that have led to the industry struggling to combat this issue. The Annex to the guidance contains a table with a list of red flags and an indication of whether those red flags might appear in open account transactions, documentary transactions, or both.

  The guidance states the importance of pooling resources and information sharing across public and private sectors including customs agencies and financial institutions, in continuing to identify trends and techniques used by criminals to launder money.

  BAFT continue to discuss the leveraging of technologies such as AI and applying data analytics can identify anomalies within data, can allow for a more targeted review of potential illicit activity.

Examples of Trade Based Money Laundering

As set out above, there are few examples of public regulatory action arising as a result of TBML. This is, at least in part, because the complex international nature of TBML and the international trade system makes investigation by regulatory authorities particularly challenging.

Example 1 – Lebanese Canadian Bank

In 2011, FinCEN cited Lebanese Canadian Bank (LCB) as a financial institution of money laundering concern, on the basis that on the basis that accounts held at the bank had been used to channel funds from drug and money laundering schemes (including TBML)

to a number of beneficiaries, including (according to FinCEN) Hezbollah. The scheme centered around purchases of second hand cars in the US – using illegal drug money sent to the US via LCB – that were shipped to West Africa and resold. At the same time, drugs from Colombia were shipped to, and sold in, Europe. The proceeds of sale of the cars and drugs were co-mingled. From there, the funds were sent to exchange houses (some of which held accounts at LCB), which diverted some of the funds to Hezbollah. Finally, LCB's network was also used to transfer funds to Asian producers of commercial goods, to be used for the purchase of goods which were shipped to Latin America and used as part of a black market peso exchange (see below for an example).

FinCEN's notice sets out that while the Bank seemed to be aware of money laundering risk (e.g. through its own risk assessment), it nevertheless permitted hundreds of millions of dollars of illicit funds to be channeled through bank accounts held by individuals suspected of involvement in drug smuggling. FinCEN went on to say that LCB's:

> "*involvement in money laundering is attributable to failure to adequately control transactions that are highly vulnerable to criminal exploitation, including cash deposits and cross-border wire transfers, inadequate due diligence on high-risk customers like exchange houses, and, in some cases, complicity in the laundering activity by LCB managers.*"

FinCEN's designation of LCB as an institution of primary money laundering concern led to civil forfeiture proceedings being taken against LCB, and the Bank eventually closed with its business being acquired by Societe Generale.

Example 2 – Black Market Peso Exchange (BMPE)

The Black Market Peso Exchange has its roots in legitimate trading activity and Colombian Government Policy. Faced with an influx of currency in the 1960s comprising profits from the coffee industry which devalued the Colombian Peso and caused financial instability, the Colombian Government enacted a law which prohibited any Colombian national from holding any currency other than the Colombian Peso. Colombians therefore had two routes to purchase goods abroad: use a bank, which was prohibitively expensive; or turn to an informal means of exchange by which Colombian Pesos were converted to foreign currency by private "brokers".

This system of exchange was exploited by narcotics traffickers wishing to launder significant volumes of currency (normally US Dollars) derived from narcotics trafficking. A narcotics trafficker provides a peso broker with a significant volume of cash, which the broker either then deposits in smaller amounts in US Banks[11], or is held by the broker to pay for goods directly. The funds are then used to purchase goods, which are shipped to South America (normally illicitly) and sold by the broker, whereupon a proportion of the proceeds of sale is remitted to the narcotics trafficker.

In a detailed and useful article on the BMPE[12] in the US Attorney's Bulletin, Evan Weitz and Claiborne Porter[13] set out a number of potential indicators for BMPE activity, including:

- structuring of deposits in round numbers, or just below the reporting threshold for payments into US bank accounts;
- deposits to accounts from multiple locations different from the area in which the account was initially opened, and/or with which the holder of the account has no obvious business link;
- significant volumes of third party payments (often across the counter) into the same account; and
- shipping significant volumes of high value goods, such as perfume and consumer electronics, to South America.

While these indicators are not exhaustive, taken together they could be indicative of an account or a series of transactions requiring further investigation.

Typologies and Red Flags

When considering whether an international trade transaction has potentially suspicious elements, financial institutions will need to consider whether the features of the transaction itself give rise to TBML concerns. As such, it will be vital for the institution to have a suite of potential indicators, or typologies, which reflect the potential risk of TBML to which it is likely to be subject.

Almost all the regulatory and industry guidance given on TBML makes reference to red flags, and many of the documents contain lists of red flags. While it is impossible to produce a truly exhaustive list of red flag indicators, set out below are examples of some of the common red flags[14] that could indicate a suspicious transaction from a TBML perspective:

1. Transaction Inconsistencies

Inconsistencies within the transaction itself can be indicative of potential money laundering risk. When considering the transaction, firms will need to be on the look-out for elements of the transaction that do not make sense in the context of the transaction as a whole, for example:

- customer due diligence processes are unable satisfactorily to verify the existence and ultimate beneficial ownership of entities or other parties involved in the transaction;
- discrepancies in the invoicing for goods and services. Examples might include the weight, amount or quality of the goods being shipped not matching known characteristics of the goods as described on the invoice;
- the market value of the goods being shipped and the overall value of the transaction are not consistent;
- no description of the goods appears on the invoice (this might indicate a phantom shipment);
- the description of the goods does not match international standards or market practice for a particular commodity (e.g. metal shipments of unusually high – or low – levels of purity);
- goods are shipped through a high-risk country when there is no obvious geographic need to do so; and
- there are numerous invoices for the same shipment of goods (this could allow multiple illicit payments, using the invoices as justification).

2. Payments and Third Parties

It will be vital, in terms of controlling TBML risk, for a financial institution to know its customers and to have carried out sufficient customer due diligence. However, even if on-boarding has taken place appropriately, red flags for TBML may arise during the transaction from transactions between related parties, or the involvement of other third parties, or the way payments are made, for example:

- payments in respect of the transaction are made by a third party or made to unrelated third parties;
- there is evidence that funds have been moved to/from accounts in high risk/sanctioned countries;
- transactions have originated from, or passed through, high risk jurisdictions;
- payment has been made of an unusual amount of money (e.g. a much higher, or lower, amount than the transaction would usually require); and

- transaction values do not correspond with a customer's known business (for example, a customer known to deal in small, low value, items suddenly starts concluding transactions for much larger value items).

3. Complex Structures

The use of unnecessarily complex structures for the transaction or in the ownership and management structures of the parties to the transaction may also be indicative of elevated TBML risk. Examples of red flags might include:

- limited information available on the purpose of the business of one or more parties;
- difficulties establishing details of the ownership of one of the parties (either direct ownership or ultimate beneficial ownership);
- suspected shell companies have been identified within the structure. Such companies exist only to reduce the transparency of ultimate beneficial ownership;
- hidden linkages between ostensibly separate parties to a trade finance transaction;
- multiple intermediaries are being used for a transaction for no apparent reason;
- involvement of businesses/parties in a particular jurisdiction is disguised (this may be the case if a transaction is linked with a jurisdiction subject to economic sanctions); and
- concealing the nature of a transaction (for example, a lack of clarity about the economic purpose of the underlying transaction for which trade finance is required). In addition to being a red flag for TBML, this may be indicative of other forms of criminality, including drug trafficking or terrorist financing.

Establishing an Effective Trade Based Money Laundering Compliance Programme

For firms carrying out trade finance activity, establishing an effective control framework addressing TBML will be key to managing legal, regulatory and reputational as risk as part of a wider financial crime compliance programme. It will be vital to ensure that any policies, procedures and controls put in place are reviewed regularly and updated as appropriate, with any changes communicated effectively to affected employees.

An effective TBML control framework will require a number of key elements:

1. A Risk Assessment – Demonstrating an Understanding of the Level of Risk in the Business

One of the central findings in the FCA's Thematic Review was that the practice of incorporating information relating to TBML risk in firms' overall risk assessments, or indeed carrying out a separate TBML risk assessment, was far from universal. The FCA noted that good practice would be for firms to document a trade finance-specific risk assessment that gives appropriate weight to money laundering risk as well as sanctions risk. It also made clear that the failure to keep such a risk assessment up to date would be an example of poor practice.

2. The importance of Knowing Your Customer (KYC)

Given the complex nature of international trade arrangements, and the TBML risk that comes alongside them, undertaking suitable customer due diligence is key to running a successful compliance programme.

Unlike traditional banking relationships, the "customer" in trade finance arrangements will vary depending on the type of arrangement being entered into. As a result, key to any KYC process is understanding which party to the transaction is, in fact, the customer. The JMLSG Guidance contains a number of sections which set out, for certain types of trade finance arrangement, who the "instructing party" is, upon whom appropriate levels of customer due diligence must be undertaken. The guidance goes on to state that where appropriate, and set out in firms' own policies and procedures, it may be necessary to undertake due diligence checks on other parties to the transaction (though the guidance recognises that the extent to which this is necessary will vary).

Where a customer or a transaction is considered to be high risk, the firm concerned will need to carry out enhanced due diligence (EDD) on the instructing party. The JMLSG Guidance explains that EDD measures in trade finance transactions may include obtaining details about the ownership and background of the other parties to the transaction, details as to the type of goods being shipped (including price paid as against market value[15]), frequency of trade, and the quality of the business relationship.

The Guidance goes on to say:

> "*The enhanced due diligence should be designed to understand the nature of the transaction, the related trade cycle for the goods involved, the appropriateness of the transaction structure, the legitimacy of the payment flows and what control mechanisms exist*."

3. Sanctions Screening

Both the Wolfsberg Guidance and the JMLSG Guidance make clear that name screening for sanctioned individuals or entities is a key part of preventing financial crime occurring through trade finance. Interestingly, the FCA's Thematic Review found that sanctions screening during trade finance transactions was among the stronger parts of firms' trade finance compliance frameworks – most likely because firms were already screening transactions for sanctions compliance in any event. The JMLSG goes on to say that where lists are available, firms should consider screening against them in real time.

Both the JMLSG and Wolfsberg guidance note, however, that although screening for sanctioned entities or individuals against sanctions lists is routinely carried out (and many firms have sophisticated electronic systems for doing so), sectoral or goods-based sanctions are far harder to implement, and will require significant expertise, and potentially a more manual approach.

4. Monitoring Customer Activity

All the guidance proposes customer activity monitoring as a key plank in the AML compliance toolkit. However, they are realistic about the extent to which automated transaction monitoring systems are able to detect potential TBML. The JMLSG Guidance makes clear that it will often be difficult to use automated systems due to the fact that the information available varies between the different types of trade finance transaction.

In open account transactions, the level of information may be as little as the identity of the buyer and seller, and the amount to be transferred, posing significant detection difficulties. Several large financial institutions are now exploring whether machine learning or artificial intelligence could be deployed as part of the overall transaction monitoring process to detect patterns in transactions

that might otherwise be missed. While this is something that could prove useful in detecting patterns of illicit activity in open account transactions, further work – and engagement with regulators around the globe – will be vital in determining the extent to which these potential solutions could make open account monitoring more effective in the future.

So while, as the guidance makes clear, the amount and depth of monitoring will depend on the risk analysis of the business or parties involved, in some trade finance transactions (particularly documentary transactions) there is still likely to be a fairly significant manual element, which may well rely on individuals in the business who are responsible for checking documents provided as part of the transaction identifying financial crime risk, based on their knowledge of the industry or of prevailing market conditions. Indeed, the FCA's Thematic Review noted the challenges to firms inherent in this model, particularly given that employees working in trade finance tended to have significant years of experience of doing so – making training of new staff all the more important in terms of the effectiveness of the controls.

5. Training

All the guidance issued by the various standard setting bodies, and the FCA's Thematic Review, make clear the importance of staff being able to access tailored training which is both directed at the staff who deal directly with trade finance issues (and those in the back office), and reflects the risks that trade finance activity represents. In addition to covering the risks of trade finance activity, the training should also cover the firm's procedures for mitigating these risks.

Blockchain – A Use Case?

Many of the inherent risks that financial institutions run in trade finance transactions – the lack of transparency of counterparties, the paper-based nature of the transactions themselves, uncertainties around the provenance and authenticity of products – could be mitigated through the use of distributed ledger technology (or "blockchain") as part of the trade finance process.

In February 2016, Barclays Bank plc released a White Paper[16] which summarised the potential for blockchain technology and its main benefits in trade finance, including:

- mitigating the risk of documentary fraud; and
- providing assurance and authenticity of products in the supply chain.

The Euro Banking Association's Information Paper "*Applying Cryptotechnologies to Trade Finance*"[17] also noted that a blockchain would offer real-time transparency in areas such as payment details, transfer of ownership, the goods themselves, and invoicing. Such transparency would go a long way towards dealing with many of the issues identified in this paper. The Paper also noted that blockchain has the potential to make the whole trade finance process more efficient, for example by improving data matching and reconciliation, enhancing dispute resolution and helping banks themselves manage credit risk by allowing for a more complete risk profile to be generated on clients.

A number of global financial institutions have invested in blockchain trade finance trials, and while at time of writing an industry standard solution seems a fair way off, the results thus far have been promising. Key to any effort to roll out blockchain solutions for trade finance more widely will be regulatory acceptance – as a result, early engagement with regulators around the world is key to ensure that they have a clear understanding of how the solution operates. In doing so it will be key to ensure regulators understand not only the benefits that these solutions may bring in terms of identifying and preventing TBML, but also any new risks to which the solutions may give rise, and how those may be mitigated.

Conclusions

Trade Based Money Laundering poses significant challenges for financial institutions, and while enforcement actions are relatively rare, studies and thematic reviews (such as that carried out in the UK by the Financial Conduct Authority) demonstrate that this is an area in which compliance with regulatory requirements has in the past been weak. And yet, international trade remains an area of significant money laundering and financial crime risk for every firm involved. While the technological solutions, and in particular the potential use of AI and machine learning, and blockchain, seem promising, it will take time to put in place solutions that are adopted widely enough in the industry to make a significant impact on money laundering through international trade. As a result, while firms still often find TBML difficult to detect – "*as if through a mirror, darkly*" – they should continue to invest in their control frameworks as part of a broader financial crime compliance programme, with a view to detecting trade based money laundering, and preventing it where possible.

Endnotes

1. Global Financial Integrity, "*Illicit Financial Flows to and from Developing Countries: 2005-2014*", April 2017, available at: http://www.gfintegrity.org/wp-content/uploads/2017/05/GFI-IFF-Report-2017_final.pdf.
2. For example, letters of credit.
3. These conditions usually relate to delivery of documentation evidencing that the goods have been shipped, such as invoices or bills of lading.
4. Wolfsberg Group, "*The Wolfsberg Group, ICC and BAFT Trade Finance Principles*", January 2017, available at: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/comment-letters/6.%20Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf.
5. See: https://www.wolfsberg-principles.com/articles/launch-trade-based-money-laundering-awareness-video.
6. UK Financial Conduct Authority, "*TR13/3 - Banks' control of financial crime risks in trade finance*", July 2013, available at: https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf.
7. UK JMLSG, Guidance – Part 2, Chapter 15, "*Trade Finance*", December 2017, available at: http://www.jmlsg.org.uk/download/10006.
8. FATF, "*Trade Based Money Laundering*", June 2006, available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf.
9. FATF Asia Pacific Group, "*APG Typology Report on Trade Based Money Laundering*", July 2012, available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf.
10. BAFT, "*TradeBasedMoneyLaundering*" August 2017, available at: http://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paperf246352b106c61f39d43ff00000fe539.pdf?sfvrsn=2.
11. Normally structured in such a way as to avoid the mandatory reporting requirement for US$ deposits over $10,000.

12. Evan Weitz and Claiborne Porter, "*Understanding and Detecting the Black Market Peso Exchange*", US Attorney's Bulletin, September 2013, p29, available at https://www.justice.gov/sites/default/files/usao/legacy/2013/09/16/usab6105.pdf.
13. Claiborne Porter is now a Managing Director at Navigant Consulting in Washington, D.C.
14. The red flags set out below reflect those appearing across guidance issued by the FCA, FinCEN, FATF and BAFT.
15. Interestingly, the Guidance suggests that if the price deviates by more than 25% from market value then further investigation may be warranted. That said, both JMLSG and Wolfsberg recognise that without knowing the precise nature of the goods and the commercial relationship between the parties, it can be extremely difficult to judge whether goods are being shipped at a fair market value.
16. Barclays Bank plc, "*Trading up: applying blockchain to trade finance*", February 2016, available at: https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/product/Banks-Trading-Up-Q1-2016.pdf.
17. Euro Banking Association, "*Applying Cryptotechnologies to Trade Finance*", May 2016, available at: https://www.abe-eba.eu/media/azure/production/1339/applying-cryptotechnologies-to-trade-finance.pdf.

Alma Angotti
Navigant Consulting
Suite 700
1200 19th Street, NW
Washington, D.C. 20036
USA

Tel: +1 202 481 8398
Email: alma.angotti@navigant.com
URL: www.navigant.com

Alma Angotti is a Managing Director and co-lead of the Global Investigations & Compliance practice. A widely recognised AML expert, she has trained and advised the financial services industry and regulators worldwide on AML and CFT compliance. Alma has an extensive background as an enforcement attorney conducting investigations and litigating enforcement actions.

Alma has counselled her clients, global financial institutions and regional institutions, in projects including gap analyses, compliance programme reviews, risk assessments, remediation efforts, and transaction reviews.

Recently, Alma held acting senior AML compliance leadership positions at global and regional financial institutions providing management of their compliance programmes and assisting them with implementing enhancements.

With more than 25 years of regulatory practice, Alma has held senior enforcement positions at the U.S. SEC, FinCEN and FINRA. As a regulator, she had responsibility for a wide range of compliance and enforcement issues affecting broker-dealers, issuers, banks and other financial institutions.

Robert Dedman
Navigant Consulting
Woolgate Exchange, 25 Basinghall Street
London, EC2V 5HA
UK

Tel: +44 207 015 8712
Email: robert.dedman@navigant.com
URL: www.navigant.com

Robert Dedman is a Senior Director in the Global Investigations & Compliance practice. He specialises in government investigations, corporate internal investigations, and anti-bribery and corruption and anti-money laundering compliance projects.

Rob has spent his career immersed in the City of London's Financial Services industry and the workings of the courts and tribunals. He also brings with him a senior regulator's perspective on the supervision of major financial institutions, along with significant expertise in investigations.

Prior to Navigant, Rob worked for the Bank of England, where from April 2013 he set up the Regulatory Action Division – the Bank of England's enforcement and supervisory intervention arm. As Head of that Division, he led the Bank of England's first ever enforcement investigations into misconduct at banks and insurers, achieving significant results against major UK financial institutions, and the first ever prohibition of a Chief Executive of a major bank.

NAVIGANT

Navigant is a publicly traded (NYSE: NCI), international consulting firm with over 5,000 professionals combining sophisticated technical skills with deep industry knowledge to provide customised services that address critical business issues. As an independent consulting firm, Navigant provides its clients with the objectivity and independence they require, without the constraints that accounting firms typically face relative to offering both public accounting and consulting services. Our team includes former senior compliance officers, bankers, accountants, regulators, prosecutors and lawyers, all of whom bring significant experience and deep expertise to help clients build, manage and protect their businesses. The Global Investigations & Compliance Practice, which comprises over 150 professionals worldwide, provides a full range of AML, CFT, anti-bribery and corruption, fraud and financial crime compliance and investigative services to clients across the globe, in the financial services industry and beyond.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com