Trade-Based Money Laundering

Your guide to understanding it, detecting it and preventing it

Trade-Based Money Laundering

Your guide to understanding it, detecting it and preventing it

Livia Benisty
Global AML Specialist, Risk, Treasury and Trade Solutions, Citi

Prior to working with the TTS AML Risk team, she worked in AML Compliance in London, where she covered TTS from an AML Advisory perspective.

Prior to joining Citi, Livia worked as a consultant on regulatory issues, advising clients ranging from large, global investment banks to hedge funds and other non-bank financial institutions.

John Ladany
Senior Market Manager – F1 Trade, Correspondent Banking Group, Treasury and Trade Solutions, Citi

John focuses on all trade-related aspects of the global Correspondent Banking Group (CBG), including export letters of credit, standby L/Cs, performance guarantees, bid bonds, reimbursements, various forms of outsourcing and the types of trade financing favored by banks. John also serves as the Global CBG Specialist for the GCC and ASEAN countries, which involves collaborating on account plans, deal structuring and support, providing clients with a senior linkage to Citi’s network and head office, and coaching and mentoring Citi’s in-country teams.

John is active in BAFT (Bankers Association for Finance and Trade), sitting on its Trade Finance Committee and is on the Administrative Board of the Pacific Rim Bankers Program.
Foreword

As financial markets and practices continue to evolve, so do the potential threats to the system. Trade-based money laundering (TBML) is one such threat, growing in sophistication and gaining increasing attention from the parties impacted by it. The uptick in TBML is primarily outside of traditional trade finance and trade services products and is most likely to creep in with open account transactions (which are less document-intensive and, therefore, less monitored and regulated, leading to a higher risk of fraud and money laundering). With open account transactions on the rise – as they are considered a cost effective (albeit riskier) replacement to traditional letters of credit – the opportunity to commit fraud and money laundering also rises.

Both financial institutions and regulators are seeking to lower the level and impact of TBML in the global markets. Joint efforts and partnerships between these two groups are essential to help reduce the instances of crime and fraud. Luckily, these efforts to diminish TBML activities are producing several avenues through which to learn about and receive guidance on combatting the risks. Within this paper, Citi experts discuss the global and regional trends of TBML and the potential impact of these trends, including illustrative TBML instances. Additionally, the team examines what specific actions are being taken by global industry participants to help identify, mitigate, and fight trade base money laundering. This paper also examines the benefits which can be achieved by implementing customer due diligence such as know your customer procedures and transaction monitoring processes.

We hope these insights will prove helpful and underscore the importance of remaining educated about TBML and the availability of detection tools and countermeasures.

John Ahearn
Global Head of Trade, Treasury and Trade Solutions, Citi
1. Global and regional trends in trade-based money laundering

Criminals are increasingly using cross-border trade to transform the financial proceeds of their illegal activities into seemingly legitimate revenues, in a process known as trade-based money laundering (TBML). Regulators are paying more attention to the problem, while banks and other firms are revising their anti-money laundering (AML) policies and procedures to take account of this growing threat.

The Financial Action Task Force (FATF), the Paris-based global body of 36 governments which co-ordinates efforts on AML and counter-terrorist financing (CTF), notes in its current version of Best Practices on Trade-Based Money Laundering that this method of laundering money has become more prevalent because banks have got better at detecting traditional methods, such as depositing cash in a bank and moving it around multiple accounts to disguise its origins. Channeling ill-gotten gains through a business transaction adds an additional layer of apparent legitimacy and opacity, thus making detection less likely.

How it works
TBML takes place in domestic as well as international trade. But it is the international trade system, with its greater complexities and vulnerabilities, that provides the best opportunities for money launderers.

The main methods are:

- Over-invoicing of goods by the exporter, so the importer transfers greater value to the exporter in the form of a payment in excess of the market value of the goods being shipped
- Under-invoicing of goods by the exporter, so the exporter transfers greater value to the importer by shipping goods of greater value than the invoice amount
- Multiple invoicing for goods, so the importer transfers more value to the exporter.
- Over- and under-shipment of goods. In the first case the exporter transfers greater value to the importer; in the second the importer transfers greater value to the exporter.
- Describing goods on the invoice and other documentation as being of a higher quality—and therefore a higher value—than they actually are, so the importer transfers greater value to the exporter.

Some real-life examples of the above are given in section 3 of this paper.

The scale of the problem
Global Financial Integrity (GFI), the Washington DC-based research company, carries out annual studies to quantify and draw attention to the seriousness of the TBML problem. In its latest report, published in December 2015, it calculates that “illicit financial flows” from developing economies between 2004 and 2013 amounted to $7.8 trillion—83% of which was due to trade based money laundering. The figure in 2013 alone, the last year for which data is available, was $1.1 trillion, more than double the amount recorded in 2004.

“This study clearly demonstrates that illicit financial flows are the most damaging economic problem faced by the world’s developing and emerging economies,” says GFI President Raymond Baker, a long time authority on financial crime. GFI estimates that these flows account for 4% of the developing world’s GDP. Sub-Saharan Africa suffered the largest illicit financial outflows in the latest study—averaging 6.1% of GDP—followed by Developing Europe (5.9%), Asia (3.8%), the Western Hemisphere (3.6%), and the Middle East, North Africa, Afghanistan, and Pakistan (MENA+AP, 2.3%).

Two other recent studies are worth mentioning. The US Department of the Treasury’s National Money Laundering Risk Assessment 2015 highlights five “vulnerabilities”, one of which is trade-based money laundering. The US Senate Caucus on International Narcotics Control report entitled The Buck Stops Here: Improving US Anti-Money Laundering Practices, published in 2013, says that trade-based money laundering is “estimated by some experts to be the largest money laundering method in use in the United States today”.

Some real-life examples of the above are given in section 3 of this paper.
2. Regulations and industry guidance on combatting TBML

There is no shortage of official recommendations, regulations and industry guidance on what banks and other firms should do to detect and prevent trade-based money laundering as a specific part of their wider AML obligations.

At the global level, the FATF has the lead, issuing advice on TBML as part of its 40 recommendations on anti-money laundering and counter-terrorist financing. It is then up to national authorities—governments, regulators and other bodies—to implement FATF’s advice, through legislation, regulations and guidance for banks to follow. In addition, industry bodies—like the Wolfsberg Group of 11 leading international banks, or the UK banking sector’s Joint Money Laundering Steering Group—offer practical suggestions for banks to act on.

A great deal of the regulatory and industry guidance on TBML focuses on how the use of such instruments as documentary letters of credit, bank guarantees and bills for collection, for example, are used in the laundering process. However, it is important to stress that most TBML takes place in open account transactions payments, through mis-invoicing and other non-finance related aspects of a transaction (as described in the “How it works section” of the previous chapter). TBML can take place in three spheres: a) within the finance documentation of a finance-supported trade, b) within the non-finance related aspects of a finance-supported trade and c) within an open account trade. About 80% of international trade is conducted on open account, and this is where the biggest TBML risks exist.

FATF

FATF’s Best Practices on Trade-Based Money Laundering is a concise, 10-page document aimed at national authorities around the world (governments, banking supervisors, law enforcement agencies, customs agencies, financial intelligence units and tax authorities) recommending how they can identify and combat trade-based money laundering.

Its best practices include the need for national authorities to:

• Provide better training to banking supervisors on how to evaluate the adequacy of banks’ policies, procedures and processes for handling trade finance activities. By “trade finance” FATF makes it clear that its use of the term includes not only the issuance by banks of letters of credit, guarantees and other trade-related documentation, but also the provision of payment services for open account trading.
• Raise private sector awareness of the problem of TBML, through conferences, seminars and other events.
• Publish “red flag indicators” and case studies to help financial institutions identify TBML activity.

FATF has also published detailed guidance for banks on this issue. In particular it provides a list of typical warning signs—“red flags”—for banks to look out for.
These include:

- Significant discrepancies between the description of the goods on the bill of lading and on the invoice. These could indicate over- or under-invoicing, over- or under-shipping or a false description of the goods.
- A shipment of goods that appears much larger than an exporter’s or importer’s regular business activity.
- Where goods are shipped through one or more countries or unconnected subsidiaries for no apparent reason.
- The method of payment appears inconsistent with the risk characteristics of the transaction.
- The types of goods shipped are deemed “high risk” for money laundering.
- The goods are shipped to, or from, a country designated as “high risk” for money laundering activities.
- The transaction involves the receipt of cash or other forms of payment from third party entities that have no apparent connection with the transaction.

**US: FFIEC**
The Federal Financial Institutions Examination Council’s (FFIEC) Bank Secrecy Act/Anti-Money Laundering Examination Manual provides guidance to officials who carry out BSA/AML and Office of Foreign Assets Control inspections. The manual includes a section on trade finance activities to help examiners assess the ability of a bank to manage the money laundering risks associated with these activities, including monitoring transactions, customer due diligence (CDD) and reporting suspicious activity.

“The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection,” notes the manual. “The involvement of multiple parties on both sides of any international trade transaction can make the process of due diligence more difficult.”

Examiners checking banks’ procedures for combatting trade-based money laundering should ensure that banks are looking out for a number of tell-tale signs, such as:

- The over- or under-valuation of goods on the invoice and other documentation.
- Partial shipment of goods.
- Shell companies or offshore front companies.

In addition, examiners should ensure that banks follow sound CDD procedures “to gain a thorough understanding of the customer’s underlying business and locations served”. This is especially important for issuing banks which, before they issue a letter of credit, should carry out rigorous CDD on both the applicant (the buyer, or importer) and the beneficiary (the seller, or exporter). The manual also says that banks should follow the guidance issued by FATF and the Wolfsberg Group.

**US: FinCEN**
The Financial Crimes Enforcement Network (FinCEN), part of the US Department of the Treasury, issues regular warnings and advice to businesses and financial institutions about money laundering linked to international trade.

For example, in October 2015 it renewed a Geographic Targeting Order (GTO), originally issued in April, to electronics exporters near Miami requiring them to follow “enhanced reporting and record-keeping” procedures. The GTO was in response to an increase in cash transactions that may be tied to trade-based money laundering schemes used by drug cartels to conceal their illicit funds.

Under the GTO the exporters have to record and report to FinCEN information about certain transactions in excess of $3,000. The information required in such cases includes the telephone number and a copy of a valid identification document of the exporter’s customer, proof of identity of any third parties involved (such as the customer’s customer) and a description of the goods and shipping details.
US: ICE
US Immigration and Customs Enforcement (ICE), which enforces federal laws on border control, customs, trade and immigration, includes AML within its remit. Its Trade Transparency Unit (TTU), based in Washington DC, was set up in 2004 specifically to combat TBML. The unit identifies global TBML trends, works with FATF and other international organizations and partners with other countries’ TTUs to analyze trade data. “One of the most effective ways to identify instances and patterns of TBML is through the exchange and subsequent analysis of trade data for anomalies that would only be apparent by examining both sides of a trade transaction,” is how ICE describes its partnerships with other TTUs.

To help analyze all the data, ICE uses a Data Analysis & Research for Trade Transparency System. This advanced, specialized computer system contains both domestic and foreign trade data and allows users in the US and partnering countries to see both sides of a transaction.

Peru is the latest country to partner with the US in this respect. ICE and the Department of Homeland Security signed a TTU agreement with Peru’s National Tax Administration in November 2015. “The TTU partnership will enhance the ability to detect TBML and other illicit trade schemes used by transnational criminal organizations and terrorist groups,” said ICE. “The new agreement will also enhance information-sharing between the United States and Peru to help prevent and investigate customs offenses.”

UK: FCA
The UK’s Financial Conduct Authority (FCA) published a report in 2013 called Banks’ Control of Financial Crime Risks in Trade Finance, based on a review of 17 banks. The review assessed how well the banks followed guidance laid down by FATF, the Wolfsberg Group and the UK’s Joint Money Laundering Steering Group (JMLSG) on the steps banks can take to identify and prevent TBML. The review found that the majority of banks in its sample, including a number of major UK banks, “are not taking adequate measures to mitigate the risk of money laundering and terrorist financing in their trade finance business”. The FCA therefore recommended that banks train their staff better, ensure that high-risk customers and transactions are identified and requisite action taken, and that they improve their management information on the issue. The FCA then explained how banks should meet these recommendations.

UK: Treasury and Home Office
Her Majesty’s Treasury and the Home Office jointly published the UK National Risk Assessment of Money Laundering and Terrorist Financing in October 2015, the first of its kind, and required under the European Commission’s AML/CTF legislative framework.

The document mentions the risks of trade finance being used by criminals and terrorist financiers to launder money, and how difficult it is for banks to monitor the problem due to the complexity of the transactions. It says that the FCA’s review of how banks control trade finance crime risks had brought the issue “to the forefront of UK banks’ risk agenda”. It adds that banks therefore need to review their operational structures and AML procedures to ensure they identify and assess money laundering risks during and after transactions.

Singapore: MAS
The Monetary Authority of Singapore (MAS) published a report entitled Guidance on Anti-Money Laundering and Countering the Financing of Terrorism Controls in Trade Finance and Correspondent Banking in October 2015. It noted that as a trading and transportation hub, Singapore is particularly “vulnerable to money laundering risks posed by trade finance”, and that the sharing of sound practices through this guidance would help banks strengthen their controls and risk management in this area.

MAS’s main recommendations are that:

- Banks should conduct a comprehensive risk assessment of their trade finance business, taking into account their customer base, geographical locations, products offered and emerging risks if any, in determining the financial crime risks they are exposed to. The MAS report makes it clear that these risks extend beyond trade finance and into areas where a bank facilitates open account trading through the provision of payment services, invoice financing, pre-shipment finance and other services.

- Banks should establish a robust due diligence process to ensure that higher risk customers and transactions are subjected to more extensive due diligence measures and closer monitoring of transactions.

- Banks should include international sanctions screening as part of their due diligence.

- Banks should become adept at checking the reasonableness of the prices of goods itemized on invoices so they can identify over- and under-invoicing.

- Banks should ensure their transaction monitoring processes and systems are robust to enable suspicious transactions to be reported.

- Banks should improve staff training on financial crime risks associated with trade finance.
In addition to recommendations from public sector bodies like FATF and national regulators, there is no shortage of advice from industry associations. The most prominent of these in respect of TBML is probably the Wolfsberg Group, the group of 11 leading international banks, including Citi.

The Wolfsberg Trade Finance Principles, which draw on FATF’s advice, give detailed guidance on how to monitor international trade transactions for signs of money laundering, with a focus on trade finance mechanisms. They cover AML guidance on letters of credit, bills for collection, guarantees, standby letters of credit and open account trading.

The Principles note how it is particularly important, but very difficult, for banks to monitor open account trading, which accounts for about 80% of world trade. “In these circumstances, unless the financial institution is providing credit facilities, the financial institution will only see the clean payment and will not be aware of the underlying reason for the payment,” it says. “The financial institution has no visibility of the transaction and therefore is not able to carry out anything other than the standard AML and Sanctions screening on the clean/netting payment.” An appendix sets out in detail how banks should monitor open account trade transactions for evidence of money laundering.

The British Bankers’ Association (BBA) regards TBML as an important area that requires the attention of its members. The BBA is a member of the UK Joint Money Laundering Intelligence Taskforce, a one-year pilot project set up by the British government in 2015 to facilitate information sharing on money laundering between the public and private sectors. Other members include the National Crime Agency, the National Terrorist Financial Investigation Unit, Her Majesty’s Revenue and Customs, City of London Police and more than 20 major UK and international banks.

The taskforce includes an operational group where bankers and law enforcement officials meet twice a week, a strategic intelligence group and an alert system. “We prioritize four areas of risk, and trade-based money laundering is one of them,” says a BBA spokesman.

The BBA has also engaged with the International Chamber of Commerce and the Bankers Association for Finance and Trade (BAFT) to help the industry, and its corporate clients, improve AML compliance standards in international trade.
3. TBML Examples

Example 1
A letter of credit was issued by Bank A in Nigeria to a beneficiary in China for the importation of seamless steel pipes valued at about $100,000. The credit was routed through Bank B. Anomalies in the documents caused them to be referred to Bank B’s Investigations Team.

The Investigations Team determined that the bill of lading issuer (B/L) was not recognized by the port loading agent, and that there was no record of the B/L number. The International Maritime Bureau was unable to obtain contact details for the B/L issuer.

Bank B returned the drawing documents to the presenter and discharged itself of the transaction.

Example 2
A letter of credit was issued by Bank A in Algeria for the purchase of around $300,000 of liquor from the UK. Bank B was asked to add its confirmation.

The goods originated in the UK, but the port of loading was in Cyprus. An “advise through” bank was specified in the Seychelles. The goods description lacked both a unit price and quantity. Subsequent communications with the beneficiary occurred via Yahoo and Gmail email addresses. The credit allowed transfer to an entity with a bank account in Lebanon.

No satisfactory information could be obtained on the concerned parties, plus the transaction structure was very unusual; it was therefore declined and the issuing bank informed. All listed parties were added to Bank B’s internal “hot list”.

Example 3
A multi-million dollar transferable letter of credit was issued by one of Bank A’s correspondent banks at the request of that country’s bureau of health. The first beneficiary, an intermediary, was to supply medical goods. Bank A was asked to confirm the credit.

The second, ultimate beneficiary presented invoices for a certain amount, and the first beneficiary substituted its invoices with a mark-up of more than 300%. The first beneficiary was a small firm with no history of multi-million dollar hospital contracts. It also appeared to have a connection with the consulting firm acting as the agent for the bureau of health.

Bank A asked the issuing bank to clarify the price discrepancies with its applicant. The initial response was vague, after which the issuing bank asserted its comfort with the transaction and asked Bank A to proceed. Instead Bank A declined, again added the various parties to their “hot list”, and considered a regulatory filing.

Example 4
This example involves 15 shell companies owned by Russians—registered in the UK, Panama, Seychelles, British Virgin Islands and Cyprus—using bank accounts in Estonia and Latvia.

The shell companies purchased goods from a well-known manufacturer of major domestic appliances and several other clients of Bank A selling high-tech electronics, metals, plastics, chemicals, apparel and other goods.
Funds derived from criminal activities funded the accounts of these shell companies, which bought the merchandise on behalf of third-party buyers. The goods were sold by Bank A’s corporate clients with minimum due diligence on the buyers, shipped to the buyers in former Soviet Union countries and then re-sold on the local markets, with the proceeds funneled back to the shell companies.

Bank A became suspicious of the transactions for several reasons: The use of shell companies registered in countries unrelated to the transactions; the use of banks in high risk jurisdictions; the global nature of the trading (the payer’s address, the payer’s bank location and the delivery address for the goods); the use of round amounts on the invoices; the use of company formation agents; and the shell companies being associated with virtual offices/ accommodation office addresses.

All of the non-client parties involved in this scheme were added to the bank’s “hot list”.

**Example 5**
At times, a preponderance of red flags in a transaction might easily be explainable and the transaction legitimate, as this example illustrates.

A jeweler (high risk business) in Kuwait (high risk country) bought diamonds (high risk goods) from a diamond district jeweler (high risk industry) in New York City. With no other details provided, four red flags were evident. However, upon further review, it was determined through publicly available information that the Kuwaiti jeweler was a well-known and reputable retailer who was legitimately purchasing diamonds for wealthy clients, in reasonable amounts, from a licensed wholesale jeweler in the US who banked with a money center institution. This due diligence sufficiently mitigated the red flags, with the residual risk considered low enough to proceed with the transaction.

As a general guideline, it is important not to escalate a trade transaction for a single red flag (such as a high risk country, product, or value) unless the transaction is obviously suspicious. If several or more red flags are present, without clear mitigating qualitative factors, then escalation is necessary to determine the legitimacy of the deal, as outlined in this Kuwait/New York City example.
So what constitutes an effective program for identifying and preventing trade-based money laundering? There are two essential components: knowing your customer, and monitoring every trade transaction.

Know your customer (KYC)/customer due diligence (CDD)
Banks must carry out checks on their customers to know who they are and their business activities. Where customers are deemed higher risk—due to their country of origin, whether they are “politically exposed persons” (PEPs) or because of some other reason—“enhanced” CDD is required. The simplified CDD procedures may vary depending on how a transaction is financed – whether it is on open account trading, a letter of credit, a standby letter of credit, a documentary collection or some other method—but in all cases the following information, based on advice from the JMLSG, should be requested:

- The customer’s owners, line of business and address, if not already known.
- The countries the customer trades with, and the trading routes used.
- The goods traded.
- The role and location of agents, banks and other third parties used by the customer in the transaction.
- Checking sanctions lists published by the US Department of the Treasury and comparable government departments in other countries to see if any of the people, companies, vessels or other entities named in the trade documents appear on these lists as what the US calls Specially Designated Nationals. If they do, it will be illegal to deal with them.

Enhanced CDD is necessary where the transaction appears to be higher risk than that normally conducted by the customer. The exercise should lead to an understanding of the transaction, the appropriateness of the transaction structure, the legitimacy of the payment flows and the control mechanisms that exist. These checks are likely to include:

- Requesting information on the ownership and background of the customer’s customer and other parties to the transaction, such as agents and shipping lines.
- Requesting information about the frequency of trade and the quality of the business relationships between the customer and the other trading parties.
- Checking the transaction against warning notices from public sources.
- Referring the transaction to external agencies specializing in validating bills of lading, commodity prices, shipping services and so on, such as the ICC’s Commercial Crime Services. This might also be accomplished internally by qualified processors tracking vessel movements through available data bases, and validating container numbers using the shipping company’s numbering algorithm.

4. Creating an effective AML program
• Checking public sources of information for the price of the goods. If the price is significantly different from the market price, consider further investigation.
• Arrange a meeting with the customer.

**Trade transaction monitoring**

A rigorous approach to monitoring trade transactions is important. Some of the details will emerge during the CDD process, but others will require specific attention. For example:

• Clear and specific AML policies and procedures must to be in place, which allow banks to identify transactions that pose higher risks of money laundering. For some countries, goods and types of businesses are higher risk than normal, and staff need to know what they are. These risks must be monitored at various stages of the transaction.

• There should be a comprehensive list of warning signs—“red flags”—for staff to look out for, such as:
  - Significant discrepancies between the description of goods on the bill of lading and on the invoice, which could indicate over- or under-invoicing, over- or under-shipping or a false description of the goods; or a shipment of goods that appears much larger than an exporter’s or importer’s regular business activity. Staff need to learn more about the price of a range of goods and services so they are better able to identify over or under-invoicing.
  - A letter of credit that fails to call for the presentation of transport documents.
  - Payment to be made to the beneficiary’s account held in a country other than its stated location.
  - Unusually favorable payment terms (such as an interest rate far above the market rate).
  - A letter of credit transferee or assignee in an offshore financial center.
  - A quantity of goods that exceeds the known capacity of the shipping container or tanker or other vessel.
  - Odd client behavior. Examples include requesting an unusual degree of confidentiality, not providing clear answers to routine commercial, financial or technical questions and approaches from an unknown third party whose identity is not clear or convincing.
  - Trade transactions need to have a description of the goods or services covered to ensure they comply with government regulations, export controls, AML requirements and other institution-specific policies. Therefore, letters of credit which merely cite a purchase order number, a contract number, a pro forma invoice number or a cryptic acronym are not sufficient and require investigation.

• Specialist staff must be assigned to the monitoring of all of these facets of trade transactions. They need to have been given sufficient and ongoing training to enable them to understand the characteristics of TBML.

• It is necessary to have good coordination between all relevant bank departments—customer management, trade finance, risk management, fraud, financial crime, compliance and internal audit. Staff in these departments need to understand each others’ roles in a transaction so they are aware of the risks, can identify suspicious activity and take coordinated action. This should be reflected in the embedded decision-making procedures governing when to escalate a transaction and to whom—from in-business controls, to the country compliance officers, and to designated global experts for AML, anti-bribery and corruption, sanctions and the like.

**Open account trading**

The JMLSG notes, as the Wolfsberg Group does, that monitoring open account trading for money laundering is especially difficult. “In open account transactions, unlike transactions where trade finance instruments are used, the bank is only aware of the payment and will not be aware of the reason for the payment, unless the relevant details are included in the associated SWIFT messages.

“Banks will therefore be able to carry out sanctions screening only on the payment, with anti-money laundering checks achieved to the extent practicable by its risk-based transaction monitoring. Where credit is being provided, however, the bank may have more information to enable it to understand the reasons for
the transaction and the financial movements. Banks are not required to investigate commercial transactions outside their knowledge, although if documentation they see as part of the banking transaction gives rise to suspicion, they should submit a SAR.”

**AML industry groups**
Banks should join one or more of the many industry and professional groups that exist that deal with money laundering issues. They are a valuable source of information, news and advice on trade-based money laundering, and provide useful forums for discussing the problem. Seeking the views and experiences of others is essential when creating and maintaining an AML program.

Some of the main organizations have already been mentioned in this paper: The Wolfsberg Group, the Joint Money Laundering Steering Group, the Joint Money Laundering Intelligence Taskforce and the British Bankers’ Association.

Others include the American Bankers Association, the European Banking Federation (EBF), the Financial Services Roundtable, the Association of Certified Anti-Money Laundering Specialists and the Bankers Association for Finance and Trade.

For example, the “2015 BAFT Canada Global Trade Finance Workshop” held in Toronto in November 2015 featured a review of the Association’s recently published document Guidance for Identifying Potentially Suspicious Activity in Letters of Credit and Documentary Collections. Presentations were given by Stacey Facter, SVP, Trade, at BAFT, and Rita Ricci, Global Head, Trade Expertise Desk, at BNP Paribas.

In addition, the “7th BAFT Global Councils Forum” held in Singapore in October 2015 featured a keynote address on how TBML is affecting trade finance as a business. In his speech Hugh Jones, the President and CEO of Accuity, the payments data provider, highlighted the nature and scale of the problem. More importantly, he explained how banks can implement effective money laundering controls while ensuring the continued growth of their trade finance departments.
5. What’s next?

In the previous four chapters we have outlined the global and regional trends in trade-based money laundering and explained the nature and scale of the problem. We have highlighted official recommendations and regulations, as well as industry guidance, on what banks must do to combat the problem. We have provided some real-life case studies. And we have described the important components of an effective TBML program.

However, in common with all forms of crime, it is an ever-present, ever-evolving threat that is impossible to eradicate. It requires constant vigilance and agility of mind from the banking industry, governments, regulators, law enforcement agencies and other public sector entities if it is to be kept in check. New ways of thinking and innovative prevention and detection tools are vital in the fight against money launderers.

So what more can be done by banks to improve their AML and CTF policies and procedures? Four things in particular stand out: the need to deploy advanced technology to take over from existing manual AML controls, institute quality assurance testing, carry out more price verification and seek further international cooperation.

Greater use of advanced technology

Bank procedures to detect TBML tend to be highly manual, with staff reading through complex trade and finance documents while looking for warning signs. Greater use of automated techniques, like optical character recognition, are being investigated. It is being used by some banks to scan through documents and look for the names of people, companies and other entities that could indicate suspicious activity and need to be vetted against the sanctions lists published by governments and multilateral agencies.

Data analytics is also a valuable tool. Global advisory firm PwC, in its 2015 report Goods Gone Bad: Addressing Money-Laundering Risk in the Trade Finance System, noted that firms are increasingly “leveraging analytics and statistical transaction monitoring techniques to identify information, trends, connections and anomalies indicative of trade-based money laundering schemes”.

Quality assurance testing

The quality of AML controls can vary significantly from bank to bank. This is even true of banks based in the same country where they are similar in culture, subject to the same regulations and have access to the same industry guidance. Regulators are, therefore, increasingly insisting that banks periodically test the quality of their AML controls. Even where regulators do not insist on this, it is good practice anyway for banks to carry out such tests.

More price verification

Money laundering reporting officers and others working in AML monitoring and control functions should learn to look for obvious over- and under-invoicing and spend more time learning price verification skills. On this second point, there is official and industry guidance stating that bank staff should become adept at checking the reasonableness of the prices of goods shown on invoices so they can identify over- and under-invoicing situations.
More international co-operation

Working together rather than working alone delivers better results. Cooperation between banks, trade associations, governments, regulators, trade transparency units (TTUs), financial intelligence units (FIUs) and other official agencies in the fight against TBML therefore needs to increase.

FATF’s Best Practices on Trade-Based Money Laundering says exactly this in relation to information sharing. It says that countries should set up ways of facilitating “the prompt and effective exchange of trade data and other relevant information...among authorized counterparts”. It further states that “countries could also be able to cooperate in joint investigations”.

The TTUs and FIUs of cooperating countries are two official portals through which such information already flows, and more is being done. The Egmont Group of FIUs, which already has 151 member FIUs, is expected to grow further in the coming years. Its stated goal is “to provide a forum for FIUs around the world to improve cooperation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field”.

BAFT, JMLSG, the Wolfsberg Group and the Joint Money Laundering Intelligence Taskforce are four of many industry groups committed to international co-operation. BAFT’s guide for identifying suspicious letters of credit and documentary collections, mentioned earlier, was written by a group of AML and KYC experts from 16 financial institutions and industry suppliers from the US, Canada, Asia and Europe. It is an example of what can be achieved through international cooperation.

“One of the challenges banks face with implementing global compliance policies is trying to interpret guidance from multiple industry bodies,” says Tod Burwell, BAFT president and CEO. “This document aims to simplify guidance from a variety of regulatory and standard setting authorities in a way that facilitates more effective policies and procedures.”

The way forward

Trade-based money laundering will never be eliminated. If anything, the threat will only continue to grow, along with the financial penalties and reputational damage to institutions that do not do their utmost to detect and prevent it. Joint initiatives like those run by BAFT and others may help to some degree. But every bank must devote the necessary time and resources to create a robust AML program for trade, to train their responsible staff, to maintain and enhance the required systems and to constantly test and verify the effectiveness of their procedures.