Combating Trade Based Money Laundering:
Rethinking the Approach

August 2017

BAFT

ACKNOWLEDGMENTS

Special thanks go to the members of the BAFT AML KYC Working Group.
This project could not have been completed without their hard work and dedication.

© 2017 BAFT, Washington, D.C., 20036

Disclaimer: This document is furnished for informational use only. Neither the contributors nor BAFT is engaged in rendering legal or other expert professional services for which outside competent professionals should be sought. All statements and opinions contained herein are the sole opinion of the contributors and BAFT and subject to change without notice.

Combating Trade Based Money Laundering: Rethinking the Approach

INTRODUCTION

In 2006, when the Financial Action Task Force (FATF) published its report, *Trade Based Money Laundering*, it was apparent that additional measures were needed to help combat money laundering and the financing of terrorism in the international trade sector. FATF concluded that "as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive" and that "the scope for abuse of the international trade system has received relatively little attention."[1]

Since that time, trade based money laundering (TBML) has become an increasing concern. A study by Global Financial Integrity estimates illicit inflows and outflows to and from developing and emerging economies was between 14–24% of their total trade from 2005–2014.[2] That is more than a trillion dollar problem—not counting the potential damage done by the use of the illicit funds. The international trade sector and regulatory agencies have worked to address the issue. FATF and other authorities have published various forms of guidance to assist banks and help other parties identify characteristics that may indicate money laundering.

BAFT (Bankers Association for Finance and Trade) established a working group to help provide clarification and guidance on the complex financial crime and know your customer (KYC) compliance requirements associated with trade finance. In March 2015, BAFT issued *Guidance for Identifying Potentially Suspicious Activity in Letters of Credit and Documentary Collections*, a comprehensive compilation of trade red flags identified by the U.S. Federal Financial Institutions Examination Council (FFIEC), FATF, the Wolfsberg Group (Wolfsberg), and the UK Financial Conduct Authority (FCA). BAFT's guidance identifies 16 distinct trade red flags.[3]

While helpful, clarification of regulations and additional compliance staff is not enough to solve the problem. The core problem with TBML is that it is a methodology criminals use to hide illicit funds by integrating them into normal commercial flows. So there is an inherent trade-off between interrupting normal commerce and intercepting illicit transactions. Some have likened this not to looking for the needle in a haystack, but rather, looking for the bad needle in a stack of needles.

---

1. FATF, Trade Based Money Laundering, June 2006.
2. *Illicit Financial Flows to and from Developing Countries: 2005–2014*, Global Financial Integrity, April 2017.
3. BAFT (2015), https://bafft.org/policy/document- library

In this paper, BAFT proposes alternative collaborative approaches to the public and private sectors for solving the problem of trade based money laundering. The objective is to increase the effectiveness of efforts to combat financial crime, while ensuring commerce through trade continues to flow in an efficient manner. We will seek to clarify misconceptions about bank-intermediated trade and the ability of banks to interdict illicit activity. We also will explore ways in which the broader group of stakeholders in international trade can better align to help reduce TBML and the financing of terrorist activities using trade.

BACKGROUND

The primary role of banks in international trade is to provide financing, risk mitigation and settlement of payment for cross-border transactions. However, they have been increasingly called upon to help identify and intercept financial crime. Banks recognize their citizenship role in protecting the integrity of the financial system, however, there are misconceptions about bank-intermediated trade and the ability of banks to interdict illicit activity.

To better understand TBML in a bank context, it is essential to first differentiate trade that is bank-intermediated from that which is not. Buyers and sellers agree to contract terms independent of any financing that may be required. In some instances, financing is not required. In other cases, financing is provided between the two parties (e.g., 30/60 day terms of sale), where the buyer pays the seller within a designated period of time from the invoice date. The only role for the bank is processing the payment to settle the transaction. The bank has no knowledge or visibility to the underlying trade transaction as it was not bank-intermediated, and therefore, has limited ability to identify illicit trade behavior.

In instances where trade is bank-intermediated, the bank may provide financing and/or risk mitigation. Financing occurs in a variety of forms including transaction types such as documentary (e.g., letters of credit, collections, guarantees) and non-documentary (e.g., trade loans, receivables/payables financing). Transactions that are non-documentary and those that are not bank-intermediated are broadly referred to as open account trade. In 2017, Wolfsberg estimated that approximately 80% of global trade was transacted using open account settlement.[4]

For documentary trade, banks observe commonly accepted rules, such as those outlined in the International Chamber of Commerce (ICC) Uniform Customs and Practices (UCP), and other similar rules for various transaction types. For documentary credits, UCP 600 Article 5 notes: "Banks deal with documents and not with goods, services or performance to which the documents may relate." For bank-intermediated open account trade, there are rules for some, but not all transaction types since financing can be very deal-specific. Deal structure and policies of the lending institution outline documentation required.

Banks receive underlying documentation for the approximate 20% that is documentary trade, a portion of non-documentary bank-intermediated trade, and 0% of non-bank intermediated trade. They are limited in both the number of opportunities to interdict illicit flows as well as the practicality of identifying "the bad needle."

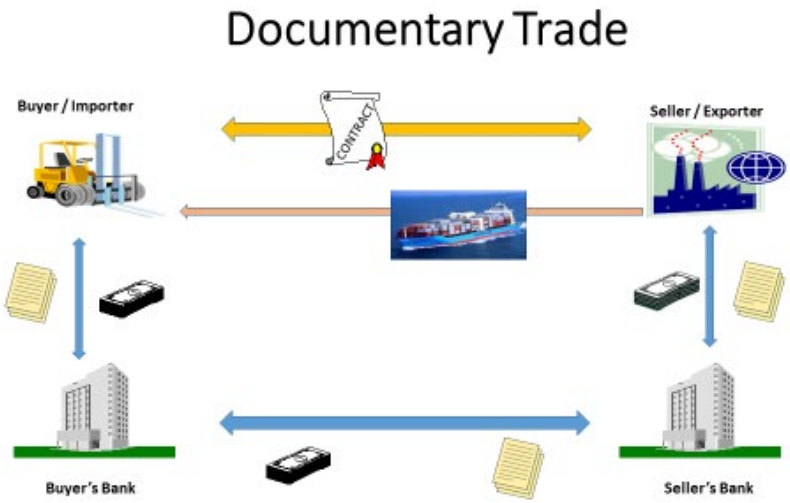
4. *The Wolfsberg Group, ICC and BAFT Trade Finance Principles 2017.*

Documentary and Non-Documentary Trade Transactions

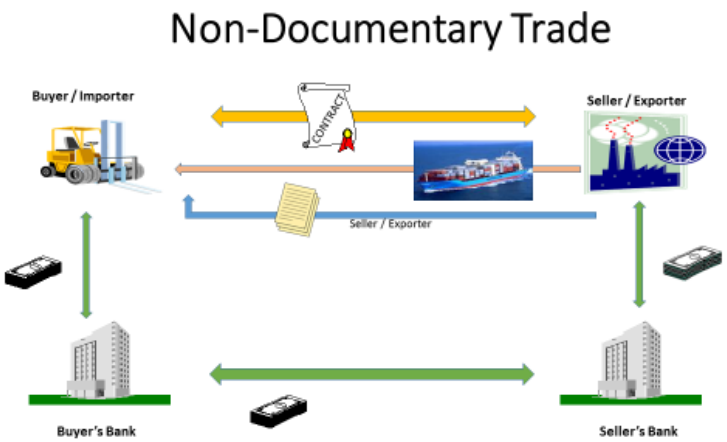
From the standpoint of an organization looking to launder illicit funds, the payment is the most important piece of the puzzle. The trade transaction, in most instances, is being used as additional cover to help avoid detection. The same way narcotics or human smuggling operations may physically co-mingle drugs or people with "normal" shipments, TBML relies on payments in settlement of trade transactions to mask the movement of illicit funds. The type of trade transaction used determines the opportunities a financial institution has to identify the suspicious activity.

In documentary transactions, the bank handles or processes documentation such as bills of lading, invoices, packing lists, etc. In non-documentary transactions, the bank may have access to only a portion of documentation based on the structure of the transaction and policy of the institution. For example, pre-shipment financing occurs before shipping documents and invoices are produced. For non-bank intermediated transactions, the bank only handles the transfer of funds without seeing any underlying documents that identify the payment as being trade related.

1. **Example of a documentary trade transaction: Processing the drawing of a letter of credit:**
   In such a transaction, to obtain payment, the seller/beneficiary presents the documents (as outlined in the letter of credit) to his/her bank. The documents may include the title/transport document, invoice, packing list, certificate of origin, inspection certificate, etc. In this case, the bank advising and/or negotiating the letter of credit has sufficient access to the transaction's underlying information to review it for red flags before executing the payment. There is some potential to identify indicators of money laundering, especially given that documents generally undergo several stages of (often manual) review by experienced processing staff within a bank's trade services department.



2. **Example of a non-documentary trade transaction: Processing a wire transfer to settle an open account transaction:**
   In such a transaction, banks usually have only the name, address and account number of the payment originator (buyer) and name and account number of the payment beneficiary (seller). The payment is typically processed without human intervention via systems in the bank's wire transfer department. It is possible that very general payment information such as "Invoice number 123," will be included, but that will not always be the case. In fact, there is rarely sufficient information about the purpose or nature of the underlying transaction to identify a payment as settlement of a trade transaction, let alone apply the red flags outlined in BAFT's comprehensive guide.



In the back of this document, Table I highlights key characteristics of different types of funds transfers and trade-related transactions that banks may handle, and how the different types of transactions determine a bank's ability to identify potential money laundering, including some of the applicable controls. Note that with funds transfers, which may or may not be in settlement of an underlying trade transaction, the bank could detect potential TBML only for that small subset of activity where supporting documentation had been requested and subsequently obtained outside of the bank's regular procedures for general funds transfer activities. Table II maps the BAFT red flags to the relevant types of payment, documentary trade and open account trade payment activity.

CHALLENGES

Typologies: Types of Money Laundering Schemes

Trade-based money laundering is defined by FATF as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin."[5] Criminals and/or terrorist organizations may try to disguise the nature of the activities they are funding or goods[6] they are shipping, to appear as normal trade transactions. Such schemes leverage the natural flow of goods in exchange for payment, to move value from one location to another without triggering suspicious activity alerts.

This paper will not address all of the various typologies used, as there have been different manifestations of TBML in different regions based on the local business practices. In general, TBML schemes may involve:

- Over or under invoicing: Misrepresenting the price of the goods.
- Multiple invoicing: Invoicing one shipment several times.
- Short or over shipping: Shipping more or less goods than invoiced.
- Obfuscation: Shipping something other than what is invoiced.
- Phantom shipping: Shipping nothing at all with false invoices.

Example 1: Over-Invoicing Price of Goods

Company A, a colluding importer in Country X, agrees to purchase 10,000 cell phones for $200 each from Company B, a colluding exporter in Country Y. The true cost of the cell phones is $100 each and the retail value of each phone is $400. Company B exports the phones and invoices Company A for $2 million, when the true value is only $1 million. Company B has just received a transfer of excess value of $1 million that MAY represent illicit funds obtained by Company A and have now been moved from Country X to Country Y. The trade documents may all be consistent with the contract and actual goods shipped, hence, without knowing the true value of the goods shipped, it is virtually impossible to detect this as TBML in the normal course of the trade transaction.

Example 2: Under-Invoicing Price of Goods

Same scenario as in Example 1, however, in this case, the contracted price of the phones is $30 each. Hence, Company A will pay Company B only $300,000 (instead of $1 million). However, when Company A sells the phones at retail, they will generate the same $4 million in gross sales, but will retain $3.7 million in profit instead of $3 million, resulting in a transfer of $700,000 in excess value from Company B to Company A.

In each case above, the technical specifications, location and brand of the phones may greatly vary the true cost. Bank personnel are typically not qualified to assess the true value/cost of goods. What if the goods

5. FATF, *Trade Based Money Laundering*, June 2006.
6. Dual-use goods are relevant in this context. These are goods that may be perfectly legitimate objects of international trade (e.g., fertilizer, cell phones, etc.) that have also been defined in various regulations as being potential components of weapons of mass destruction (WMDs). Financial institutions are required to flag trade transactions with indicators of a criminal scheme involving WMDs as well as those with indicators of money-laundering, but the same limitations that apply to screening for TBML apply to WMDs.

shipped are actually narcotics instead, but the invoices and shipping documents state cell phones? How would the bank know, since they only deal in documents, not the actual goods? What if the invoices are submitted and paid multiple times? What if the invoices are submitted and paid, but no shipments actually take place? All of these represent TBML schemes, and a bank's ability to identify red flags also depends on whether it is bank-intermediated trade and if documentary or non-documentary settlement methods are used.

Over 80% of the time, Company A and B settle transactions such as this on open account, limiting banks' ability to even identify the payment as settlement of a trade transaction. Only in cases where banks are financing the open account trade transaction would they know of its existence. Open account settlements are typically handled by wire transfer or checks. Some open account activity may be handled through "netting," where the buyer and seller have multiple transactions between them and may owe each other money. Rather than issuing multiple individual payments, the parties may agree to settle via a single net payment. Netting of payments can further obscure the nature of the transactions.

If the transaction was settled using documentary trade (e.g., letter of credit), then the processing staff might notice anomalies if the documentation was inconsistent. If the bank were providing post-shipment financing, they might also have access to some documentation. However, it is also feasible that the true unit cost of a cell phone is $100, or $200 or $30, thus making the red-flag for over/under invoicing very difficult to detect. Similarly, banks deal only in documents, so they are not positioned to determine if the shipment actually contained 10,000 phones, some other quantity, or something other than cell phones.

There is limited data to indicate what percentage of actual TBML involves bank-intermediated, documentary and non-documentary trade. Nevertheless, for reasons outlined above, there appears to be a very low instance of documentary TBML relative to open account. Yet, an inordinate amount of emphasis is placed on the controls within the trade services department to mitigate TBML in documentary trade.

More than US$3.07 quadrillion in payments are made annually.[7] By comparison, World Trade Organization (WTO) estimates roughly $16 trillion of trade transactions occur each year. Accordingly, approximately 0.52% of the value of all payments represent trade settlement. Given that at least 80% of trade is open account, only about 0.1% of the value of payments made reflect settlement of documentary trade. **All of the AML monitoring and controls put in place in a bank's trade services department are there to identify and intercept roughly 0.1% (or less) of illicit funds flow.** This is not a very efficient use of resources.

To truly make a difference in mitigating TBML, we must look beyond documentary trade, and beyond banks.

7. CHIPS and the World Bank, 2015.

Monitoring Non-Documentary Trade Transactions

Banks are expected to understand their customers and their customers' business. A due-diligence assessment of a corporate client at the time of onboarding may include expectations of volumes, values and trade flows as well as an understanding of the types of goods and services involved. This customer profile allows banks to periodically validate that the transaction flows are consistent with the business profile of the customer. If a dairy company starts transacting in precious metals, a red flag may be raised either during the processing of a transaction, or in post-transaction reviews if they used documentary trade settlement.

If a bank customer that conducts international trade only uses the bank to settle its transactions (i.e., does not use the bank's trade services), the bank does not have opportunity to identify changes in underlying trade flows, only changes in payment flows. A company with annual turnover of $10 million that makes and receives $15 million in payments in a given month, may raise a red flag in periodic client reviews. Large companies may transact with thousands of counterparts around the world, so it becomes even more difficult to identify and monitor changes in a company's counterparts. When a bank sends a payment on behalf of its corporate customer to a beneficiary at a foreign bank, the U.S. bank may have very limited information on the receiving bank's customer.[8]

Most wire transfers flow straight through bank systems electronically, without manual intervention. For some intermediary banks, less than 5% of transactions are seen by bank personnel. However, even when wire transfers do not flow straight through the system and must be reformatted, the transfer instructions may not include explicit details on the purpose of the transfer. This information might also be transmitted from the originator to the beneficiary outside the wire transfer (e.g., by email), and outside of bank systems.

Even when wire transfers do contain details on the purpose of the payment, the financial institution does not have any documents to validate. The details themselves offer little for analysis, such as:

1. Payment for settlement
2. Payment for invoice 1234
3. Payment for goods
4. Payment for 1000 widgets as per invoice no. 1234

Generally, the only time a bank intervenes to obtain more details on a payment is if:

1. The payment instructions are unclear, requiring more information.
2. A sanctions filter automatically stops the transaction for further review by Operations and/or Compliance staff. The bank may ask for additional detailed information on the underlying transaction and purpose of the payment to determine if there is actually a true "hit" i.e., a sanctions violation.

8. According to FATF's October, *2016 Guidance on Correspondent Banking*, "To clarify, the FATF Recommendations do not require financial institutions to conduct customer due diligence on the customers of their customer (i.e., each individual customer)."

Banks periodically conduct post-transaction reviews, which may offer opportunities to identify TBML activity. Such post-transaction reviews are typically run on a monthly basis, and may leverage predefined algorithms and parameters to identify patterns of activity that may be deemed "unusual." Unusual activity is not necessarily suspicious or criminal, and institutions follow a review and escalation process to assess whether a Suspicious Activity Report (SAR) should be filed or other course of action taken. Post-transaction reviews can help identify TBML, but are limited by the scope, type and quality of data that can be analyzed and validated.

A bank may potentially spot red flags and issue a trade-related SAR only when documentation reveals the nature of the trade. Between March 1, 2012, and December 31, 2016, U.S. TBML/BMPE (Black Market Peso Exchange) SAR filings represented less than 1% of overall U.S. SAR filings.[9] FATF notes that most jurisdictions do not identify TBML as a separately identifiable activity, that is, something apart from money laundering in general.[10] Such identification would generate better statistics and information on TBML.

Better data and reporting on TBML SARs would help localize the actual risk and points of vulnerability, but from the above, it should be fairly obvious that the highest likelihood of successfully achieving TBML is through open account non-bank intermediated trade. Hence, piling more checks and controls to interdict documentary trade transactions is not likely to produce a material impact on TBML. Our attention, therefore, should look beyond bank trade services operations and examine other approaches to increase effectiveness of stopping this illicit activity.

SOLUTIONS

A starting point for all stakeholders is continuous education, awareness, procedures and compliance discipline. We take these as a common baseline, though we recognize not all institutions have the same level of expertise or systematic capabilities. As technology continues to evolve rapidly, more tools to combat TBML are available. Unfortunately, criminal organizations are always working to stay one step ahead, often utilizing some of the same technology. Nevertheless, as we characterized the problem as one of finding the bad needle in a stack of needles, organizing the solution requires collaboration, analytics and a targeted approach.

Information Sharing

Partnering and information sharing has been instrumental in combatting TBML. It is understood that data sharing and privacy concerns must be weighed, and this has been flagged as one of the obstacles to more effective efforts to combat financial crime. That issue may be explored in more detail in other papers, but there is a practical example of how that can help the industry better combat TBML.

Started as a 12-month pilot project in 2015, the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) established itself as a successful AML public-private partnership led by law enforcement and included several

9. FinCEN Suspicious Activity Report (Form 111) Exhibit 4, Number of Filings by Type of Suspicious Activity by Depository Institutions, March 1, 2012–Dec. 31, 2016

10. FATF, *Best Practices on Trade-Based Money Laundering*, June 2008.

government agencies, the British Bankers Association, UK and international banks. Its aim was to improve intelligence sharing to aid the fight against money laundering. The inter-agency operation has been so successful, it is now a fully established dimension of UK anti-money laundering strategy. As JMLIT continues to demonstrate successful prevention and prosecution of financial crime, the UK National Crime Agency (NCA) continues to "[work] with colleagues from overseas law enforcement agencies to help inform the development of similar partnerships.[11]"

Such a public-private partnership has tremendous value in identifying trends as information is able to be shared in a controlled setting that may not be detected just within one institution. Further, by highlighting evolving trends, it enables all participants to be more targeted, and thus more effective. It also demonstrates an intangible, yet very valuable point that law enforcement, government agencies and financial institutions are all on the same team when it comes to fighting financial crime. Other governments have looked at the JMLIT and are considering the value of such efforts in different countries. We believe such public-private partnerships must be encouraged and supported.

When FATF published[12] its list of trade red flags, it included a broad range of trade-related activity and the involvement of parties other than banks. As outlined by FATF, shipping companies, shipping agents, freight forwarders, customs brokers and customs officials also may be involved in handling trade transactions and also have a role to play in identifying TBML activities.

Keep in mind that only 20% of all trade is documentary, only 0.1% of the value of all payments are settlement of documentary trade. The TBML net must be cast much wider than just banks. For instance, customs clearance is a vital check point where all goods entering a country must have proper classification, valuation and inspection in order for a buyer to claim them. This process serves a variety of economic and national security interests, and can also be a vital point of intersect to combat TBML. A JMLIT-type of partnership should include the customs and freight community, as well as the financial community.

Data Analytics

Banks and government entities have invested heavily in technology to improve their ability to identify anomalies in payments, non-documentary and documentary trade. It is worth noting here that certain types of data analytics have been highly successful when used by government to identify and combat trade-based financial crime. As described in a 2016 Congressional Research Service Report[13]:

> "Within the U.S. Department of Homeland Security (DHS), Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI) established the first Trade Transparency Unit [TTU] in Washington, D.C., in 2004. Using a specialized computer

11. http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit
12. FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, 2012, updated October 2016.
13. CRS, Trade-Based Money Laundering: Overview and Policy Issues, 2016, p. 13-14.

> system called the "Data Analysis and Research for Trade Transparency System" [DARTT], TTUs examine trade anomalies and financial irregularities in domestic and foreign trade data to identify instances of TBML, customs fraud, contraband smuggling, and tax evasion …. According to one estimate, more than $1 billion has been seized since the creation of the U.S.-and foreign-based TTU effort."

What the TTU was able to achieve was an aggregation of data across all shipments to analyze price variations outside of a range, thus allowing for a more targeted review of potential over/under invoicing. This is a much more effective approach than relying on individual bank personnel at different institutions, and was instrumental in helping law enforcement identify and apprehend criminal organizations utilizing different TBML methods. It is important to note that using customs data was central to the TTU. This is a much more comprehensive and reliable source of price valuation analytics than bank trade services personnel.

An integrated combination of data analytics from customs, shipping and freight companies, and financial institutions, could offer a vastly improved ability for law enforcement to identify patterns of illicit behavior, illicit flows, and have a material impact on interdicting TBML.

Emerging Technology

With the introduction of distributed ledger technology (DLT), we have seen banks and the FinTech community feverishly at work trying to apply the benefits of the technology to solve business problems. One such problem involved the duplicative (fraudulent) discounting of receivables. In the Qingdao case in 2014, companies were alleged to have used warehouse receipts for the same metals stockpiles several times to commit hundreds of millions of dollars of fraud. A proof of concept run by banks in Singapore demonstrated that DLT was able to mitigate the multiple invoicing fraud problem. While the limited case demonstrated the capability of the technology, the industry still faces the challenge of widespread availability, adoption and deployment else, a company that tries to commit fraud at one institution will try again at others until they succeed.

Artificial intelligence (AI) and cognitive computing have emerged as promising technologies that learn and adapt as more information is provided. This is valuable to all stakeholders to be able to identify complex patterns, both in post-transaction audits, and in predictive models, which is even more powerful. We see examples of this currently helping to mitigate credit card fraud—often in real time. Market leaders are actively assessing applications for advanced technology to improve their ability to detect and mitigate illicit behavior, but we are still early in the cycle.

Emerging technology can help in the fight against financial crime, but as it evolves, taking a coordinated, risk-based approach is still paramount. Data pooling across stakeholder communities (public and private) may be more effective than organizations deploying duplicative solutions. Organizations are already constrained by funds available for investment in technology, so shared investments in such data pooling solutions can also reduce the cost, risk and potentially accelerate the timeline for deploying technology solutions to mitigate financial crime. Smaller organizations are more likely to be most constrained in their ability to make significant technology investments. Consideration must be given for how capabilities in that part of the global trade and financial ecosystem can be bolstered.

CONCLUSIONS & RECOMMENDATIONS

The problem of TBML is significant and difficult to detect. Like most forms of money laundering, sophistication of structuring and the ability to co-mingle illicit transactions with legitimate transactions makes it very difficult to detect. Transactions are stitched together in a way where individually, they may appear on their face to be legitimate, and can only be detected when looked at across a broad spectrum to identify the illicit pattern. That includes looking beyond a single financial institution's transactions. That includes looking beyond financial institutions collectively.

There are many misconceptions about TBML, which has inhibited the industry's effectiveness in combatting it.

1. Most TBML occurs in non-documentary trade, and trade settlements represent only 0.1% of the value of all payments. Layering additional controls on the manual operations in a bank's trade operation will not solve TBML. The solution must reach beyond banks. Law enforcement, government agencies and regulators should take an ecosystem approach to this problem, bringing together financial institutions, customs agencies, shipping companies and other stakeholders that have access to different information. In this way, an end-to-end view can be constructed, and mitigating controls put in the right place.

2. Information sharing across public-private sectors is vital to identifying trends, structures and techniques used by criminals, thus improving the ability to combat TBML. By gathering and sharing relevant information through a codified process, stakeholders can better identify TBML.[14] The UK's JMLIT is a good example of partnerships between government, regulators, law enforcement, financial intelligence units (FIUs) and business. These types of cooperative partnerships that can examine current case studies and trends, should be considered in jurisdictions where TBML is a concern, as this can help mitigate the contagion of TBML schemes used across multiple institutions.

3. Data pooling, particularly including data from customs and the freight community, is vital to the analytics to detect TBML methods such as over/under invoicing. Banks are just one node on the network used by criminals, and do not have all the necessary data to identify and interdict TBML. Pooling data across stakeholders will allow for more robust analytics and higher success. The TTU concept should be considered as a means to pool data in a protected manner to identify anomalies, helping to better target law enforcement investigations. While this is currently a government run system, deploying public-private solutions of this nature will be much more effective. It is important to recognize that individual institutions and industries have limitations, but an ecosystem view allows for a more effective means to detect and proactively prevent financial crime.

4. More comprehensive and globally consistent SAR classification and tracking will aid in the analysis of the TBML problem. More consistent standards across jurisdictions, better data on measuring and qualifying the problem and success of solutions is needed. Enhancing existing classification systems to improve identification of anomalies could assist various stakeholders with the current challenges in detecting and investigating suspicious activity.

14. Considering the limitations related to sharing information and data related to privacy and confidentiality rules, stakeholders must consider how to share data effectively.

5. Better education is needed across all stakeholders. There are many gaps in understanding what information is available to parties across the disparate and unconnected value chain, and at what points in a transaction cycle. Many redundancies exist along with many gaps, leading to higher costs and inefficiencies. The public and private sectors, including multiple industry players/stakeholders, must work together to fill the gaps in understanding, and leverage each other's expertise and position in the transaction cycle. Again, this could be achieved through a cross-industry public-private partnership as suggested above.

6. New technology should continue to be evaluated for its usefulness, and where appropriate, leveraged for purposes of combatting TBML. Pooled/shared investment should be considered to ensure that the broader ecosystem is utilizing the most advanced methods to identify and interdict financial crime, while minimizing the duplicative cost to each institution. Smaller and less sophisticated institutions must also have access to technological solutions, else, they will become the main targets for entry into the financial system by criminal organizations.

The success of financial crime compliance initiatives should consider the effectiveness of outcomes, not just adherence to a process. Financial institutions continue to go to great lengths and dedicate significant resources to identify TBML, and have no appetite to facilitate illegal activity. They must remain aware, disciplined, and vigilant when it comes to methods and tools to identify, report and interdict financial crime. However, financial institutions are highly limited in their ability to combat financial crime. These roadblocks present challenges in detecting TBML, terrorist financing and the proliferation of WMDs. To impact the effectiveness of anti-TBML efforts, we must include, but look beyond banks.

Initiatives such as the JMLIT and the TTU have demonstrated that both gathering wider information across the industry and applying data analytics can result in much more successful identification and prosecution of criminal activity. We are aware of efforts in other jurisdictions to consider more integrated public-private sector trade platforms. Development of better forums for sharing such information (both formally and informally) might result in creation of better red flags and typologies for all parties to be able to enhance their ability to identify potentially suspicious activity.

BAFT looks forward to continuing the dialogue with governments, industry, regulatory bodies and other associations working to help combat money laundering. We stand ready to assist in the further development of an advocacy and educational campaign on behalf of the industry to help build and maintain a better understanding of the nuances in TBML.

TABLE I:

Transaction Types, Information Normally Available, the Potential For Detecting Documentary Trade Based Money Laundering and Typical Controls Applicable to Each Transaction

Transaction type	Is there an underlying trade transaction?	Potential for detecting Documentary TBML?	Do banks see trade documents?	When might a bank see underlying documents?	Controls may include: (See note at the foot of the table)
Check payment	Possibly	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment
ACH payment	Possibly	No	No	Only if specifically requested as part of a post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment
International ACH Transaction (IAT)	Possibly	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment • Potential Sanctions screening (not required for domestic U.S. ACH)
Funds Transfer (RTGS – Real Time Gross Settlement payment)	Possibly	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment • Check for completeness of payment details (depending on local regulatory requirements)
Bank-to-Bank Reimbursements	Yes	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment
Clean collection	Possibly	Yes	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds
Documentary collection	Yes	Yes	Yes	Always	• Sanctions screening of names appearing in documents
Guarantees	Yes	Yes	Not unless specified under the terms of the guarantee	Depending on the type of guarantee	• Credit approval • Sanctions screening at issuance • Document review (including sanctions and red flags review) for payment
Standby Letter of Credit	Yes (in some cases)	Yes	Not unless specified under the terms of the standby	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Credit approval • Sanctions screening at issuance • Document review (including sanctions and red flags review) for payment
Documentary Letter of Credit	Yes	Yes	Yes	Always	• Credit approval • Sanctions screening at issuance • Document review (including sanctions and red flags review) for payment and negotiation
Supply chain finance	Yes	Yes	Depends on the terms of the transaction	Unless required under the terms of the financing arrangement, documents would only be seen in the event of a sanctions or monitoring trigger	• Credit approval • Sanctions screening of names received in documentation/ electronic data received • Sampling and verification of underlying transaction
Bank Payment Obligation	Yes	Yes	No, instead of documents the bank is involved in data matching	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Credit approval • Sanctions screening of names received in documentation/ electronic data

Unless noted in the controls column in the table, real time sanctions screening of the payment should be in place for all products. Banks may also include information about whether a client uses a particular bank product in their due diligence files and also may conduct post transaction AML monitoring on account activity.

TABLE II:

Mapping of BAFT Red Flags to Payments, Open Account Trade Payments and Documentary Trade Transactions Including Payments

	BAFT Red Flags	Payments	Open Account Trade Payments	Documentary Trade Transactions including payments
1	The customer engages in transactions that are inconsistent with the customer's business strategy (e.g., a steel company that starts dealing in paper products) or make no economic sense.		X[15]	X
2	A customer deviates significantly from its historical pattern of trade activity (i.e., in terms of markets, monetary value, frequency of transactions, volume or merchandise type)	X[16]	X	X
3	Transacting parties appear to be affiliated, conduct business out of a residential address, or provide only a registered agent's address	X[17]	X	X
4	Customer conducts business in jurisdictions that are at higher risk for money laundering, terrorist financing or other financial crimes	X[18]	X	X
5	Customer shipping items to, through or from higher money-laundering risk jurisdictions including countries identified by the Financial Action Task Force as "non-cooperative jurisdictions" in regards to anti-money laundering regulations			X
6	Customers transacting in activities/goods that potentially involve a high risk of money laundering and other financial crimes including activities/goods that may be subject to export/import restrictions		X[19]	X
7	Obvious over or under pricing of goods			X
8	Obvious misrepresentation of quantity of goods shipped			X
9	The payment terms or tenor are inconsistent with the type of goods			X
10	Transaction structure and/or shipment terms appear unnecessarily complex or unusual and designed to obscure the true nature of the transaction			X
11	The LC contains non-standard clauses or phrases or has unusual characteristics			X
12	The LC is frequently significantly amended for extensions, changes to the beneficiary and/or changes to the payment location			X
13	The transaction appears to involve use of front or shell companies for the purpose of hiding the true parties involved			X
14	The bank is approached by a previously unknown party whose identity is not clear, who seems evasive about its identity or connections, or whose references are not convincing, or payment instructions are changed at the last minute			X
15	Trade-related documentation under an LC or documentary collection appears illogical, altered, fraudulent, or certain documentation is absent that would be expected given the nature of the transaction			X
16	Transaction involves obvious dual use goods			X

15. Such as goods description codes, if established as a baseline for the client.
16. Beneficiary's country, if shown; amounts/volumes outside transaction averages.
17. Originator and beneficiary are similarly named.
18. For example, if the beneficiary's country is shown, and it appears on FATF's list of high risk and non-cooperative jurisdictions.
19. Customer's type of business per KYC record.

GLOSSARY OF TERMS

ACH payment
An electronic batch payment system that may or may not feature same-day settlement. Examples of ACH systems include the ACH in the U.S., BACS in the UK, and ECG in Hong Kong.

BAFT
BAFT is a leading international financial services trade association that helps bridge solutions across financial institutions, service providers and the regulatory community. It engages on a wide range of topics affecting transaction banking, including trade finance, payments and compliance.

Bank-to-Bank Reimbursement
A type of payment reimbursement under a documentary letter of credit whereby the bank issuing the documentary letter of credit authorizes a third bank ("reimbursing bank") to honor reimbursement claims made by the nominated bank under the documentary credit.

Bank Payment Obligation
An irrevocable undertaking given by a bank to another bank that payment will be made on a specified date after successful electronic matching of data according to industry-wide ICC rules.

CHIPS
The Clearing House Interbank Payments System is the largest private-sector U.S.-dollar funds-transfer system in the world, clearing and settling an average of $1.5 trillion in cross-border and domestic payments daily.

Clean collection
A "Clean Collection" means the handling by banks of financial documents, in accordance with instructions received, in order to: (1) obtain payment and/or acceptance, or (2) deliver financial documents against payment and/or against acceptance, or (3) deliver financial documents on other terms and conditions.

CRS
The Congressional Research Service (CRS) works exclusively for the United States Congress, providing policy and legal analysis to committees and Members of both the House and Senate, regardless of party affiliation. CRS is a legislative branch agency within the Library of Congress.

Documentary collection
A "Documentary Collection" means the handling by banks of commercial documents, which may or may not be accompanied by financial documents, in order to: (1) obtain payment and/or acceptance, or (2) deliver documents against payment and/or against acceptance, or (3) deliver documents on other terms and conditions.

Documentary letter of credit
An unconditional undertaking, given by a bank (the "Issuing Bank") at the request of their customer (the Applicant or Importer) to pay the Beneficiary (or Supplier) against stipulated documents, provided all the terms and conditions in the Letter of Credit are complied with.

FATF
The Financial Action Task Force, established in 1989, is an intergovernmental organization that sets standards and promotes legislation as well as regulatory reform to combat money laundering, terrorist financing and other related threats to the international financial system.

FCA
The UK Financial Conduct Authority regulates the conduct of more than 56,000 financial services firms and financial markets and is the prudential regulator for over 18,000 of those firms. Its aim is to protect consumers, protect and enhance the integrity of the UK financial system, and to promote competition.

FFIEC
The Federal Financial Institutions Examination Council is a formal interagency body empowered to prescribe uniform principles, standards and report forms for the federal examination of financial institutions and to make recommendations to promote uniformity in the supervision of financial institutions. The FFIEC receives its authority from the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB).

FinCEN
FinCEN is a bureau of the U.S. Department of the Treasury. The Director of FinCEN is appointed by the Secretary of the Treasury and reports to the Treasury Under Secretary for Terrorism and Financial Intelligence. FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.

Global Financial Integrity (GFI)
Global Financial Integrity is a non-profit, Washington, DC-based research and advisory organization, which produces analyses of illicit financial flows, advises developing country governments on effective policy solutions, and promotes pragmatic transparency measures in the international financial system as a means to global development and security.

Guarantees
An undertaking given by a bank (guarantor) on behalf of its customer (applicant) to another party (beneficiary) to pay a stated sum of money if the customer fails to comply with a contractual obligation. The bank undertakes to pay a stated sum of money against presentation of specified document(s) in compliance with the terms of its guarantee.

International ACH (IAT) Transaction
A (US$) debit or credit entry that is part of a payment transaction involving a financial agency's office that is not located in the territorial jurisdiction of the United States. Source NACHA.

RTGS payment
A gross settlement system in which both processing and final settlement of funds transfer instructions can take place continuously (i.e., in real time). Source: Basel Committee on Banking Supervision. Examples of RTGS systems include Fedwire, CHIPS and TARGET.

Standby letter of credit
A standby letter of credit is a guarantee of payment issued by a bank on behalf of a client that is used as "payment of last resort" should the client fail to fulfill a contractual commitment with a third party.

Supply chain finance
The use of financing and risk mitigation practices and techniques to optimize the management of the working capital and liquidity invested in supply chain processes and transactions. SCF is typically applied to open account trade and is triggered by supply chain events.

Wolfsberg
The Wolfsberg Group is an association of 13 global banks that aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

Working Group
The BAFT AML KYC Working Group (Working Group) includes experts in trade finance and compliance from BAFT's financial institution and supplier membership. Its mission is to assist in providing guidance and clarification on the complex financial-crime compliance requirements associated with trade finance activities.

1120 Connecticut Avenue, NW
Washington, DC 20036, USA
Website **BAFT.org**
Phone **+ 202-663-7575**
Fax **+ 202-663-5538**

BAFT