A Financial Institution Risk-management Framework to Mitigate Trade-Based Money Laundering

CAMS-FCI Advanced Certification Programme 2019

Michael. A. Dunlop
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>DEFINITIONS AND REGULATORY PRINCIPLES</td>
<td>3</td>
</tr>
<tr>
<td>UNDERSTANDING GLOBAL TRADE</td>
<td>5</td>
</tr>
<tr>
<td>THE PSYCHOLOGY OF FRAUD AS A PREDICATE OFFENCE TO TBML</td>
<td>6</td>
</tr>
<tr>
<td>RISK CLASSIFICATION AND CHALLENGES IN TRADE FINANCE</td>
<td>8</td>
</tr>
<tr>
<td>POSSIBLE HIGH-RISK INDICATORS OF TBML</td>
<td>9</td>
</tr>
<tr>
<td>SOFTWARE SOLUTIONS AND APPLIED ANALYTICS</td>
<td>12</td>
</tr>
<tr>
<td>RISK MANAGEMENT FRAMEWORK AND INTERNAL CONTROLS</td>
<td>14</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>16</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>18</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

Money laundering is corrosive to society and detrimental to sound business principles. As emerging economies open their financial markets, money laundering will become more attractive to criminal organizations seeking to integrate their ill-gotten gains. Trade finance is a key contributor to driving a sustainable economy, and therefore, jurisdictions engaged in legal trade and trade finance could be significantly impacted if Financial Institutions (FIs) do not have robust controls and systems to mitigate the risks of money laundering, sanctions evasion, and terrorist financing.

The purpose of this white paper is to illustrate the existing challenges FIs face from evolving organized crime, and to recommend the enhancement of Operational Effectiveness (OE) and robust controls, along with the use of an Intelligence-Led Financial Crime Risk Management framework, to mitigate Trade-Based Money Laundering (TBML). Therefore, setting a strong compliance culture is imperative. FIs should adopt a Risk Management Framework (RMF) consisting of the combined use of applied analytics, artificial intelligence, robust financial crime controls that are regularly tested, and effective human investigation capabilities to mitigate TBML in order to meet regulatory obligations, while simultaneously enhancing the customer experience aligned to a safe growth strategy.

DEFINITIONS AND REGULATORY PRINCIPLES

Where criminal activity generates significant wealth, the primary objective of the individual or group is to control the funds in a way that attracts less attention from authorities. To avoid investigation, criminals generally attempt to disguise the illicit sources through the legitimate financial system. This activity is called “laundering,” as the process attempts to turn “dirty” money into “clean” money. Interpol defines the term “money laundering” as, “any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources.” As a consequence, it is estimated that money laundering accounts for 3–5% of the global GDP and aids the facilitation and continuity of criminal organizations and terrorism. Subsequently, one of the new frontiers in enhanced money laundering enforcement is the phenomenon of Trade-Based Money Laundering (TBML).

TBML is the “process by which criminals use a legitimate trade to disguise their criminal proceeds from their unscrupulous sources. The crime involves a number of schemes in order to complicate the documentation of legitimate trade transactions; such actions may include moving illicit goods, falsifying documents, misrepresenting financial transactions, and under- or over-invoicing the value of goods.” It is understood that this form of criminality may be difficult to initially detect, and the proceeds of crime may enter the FI monetary system and be layered prior to integration.

The Financial Crimes Enforcement Network’s (FinCen) definition of an FI includes any person doing business in one or more of the following capacities:

1. bank (except bank credit card systems);
2. broker or dealer in securities;
3. money services business;
4. telegraph company;
5. casino;
6. card club;
7. a person subject to supervision by any state or federal bank supervisory authority.\textsuperscript{5}

For the purposes of this white paper, the scope of an FI will be limited to a bank. In the United Kingdom (UK), for example, the National Crime Agency (NCA) estimated that hundreds of billions of pounds related to proceeds of crime are laundered through UK banks each year.\textsuperscript{6} As a result of the risks associated with TBML, international law enforcement enhanced methods of addressing the issues and implemented regulations for FIs.

The Wolfsberg Group is an association of 13 banks that aims to develop a framework and provides guidance for the management of financial crime risks, including: Know Your Customer (KYC), Anti-Money Laundering (AML), and Counter Terrorist Financing Policies (CTFP). The group has published numerous advisory to provide FIs a perspective on effective financial crime risk management.\textsuperscript{7} Therefore, the Wolfsberg Group’s Trade Finance Principles were issued in 2017 with the International Chamber of Commerce (ICC) and the Bankers Association for Finance & Trade (BAFT).\textsuperscript{8}

The Financial Action Task Force (FATF) is an inter-governmental and policy-making body whose objectives are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other threats to the integrity of the financial system. Alongside their recommendations to combat money laundering, FATF published a TBML Report in 2006, which identified three major methods used by criminal organizations and terrorist financiers to move money for the purpose of disguising its origins and integrating it into the legitimate economy.\textsuperscript{9} A second publication from The Asia/Pacific Group (APG) regarding typologies on TBML (2012) updates and extends the FATF study by identifying red flags to detect and respond to TBML; identifying current methods and techniques of TBML; and considering why so few TBML investigations and prosecutions have been undertaken since the initial report in 2006. FATF, the Wolfsberg Group, and the Joint Money Laundering Steering Group (JMLSG) have continuously highlighted the misuse of international trade finance as a common typology used by criminal organisations and financiers of terror to enhance the cross-border flow of illicit money, aiming to integrate the proceeds into a legitimate economy.\textsuperscript{10}

In July 2013, the UK Financial Conduct Authority (FCA) Thematic Review on “Banks’ control on financial crime risks in trade finance” documented that, “Trade finance is a key component in maintaining a competitive and productive economy.”\textsuperscript{11} “London’s position as a major financial centre could be severely affected if FIs engaging in trade finance activity do not have appropriate systems and controls to prevent money laundering, terrorist financing and sanctions breaches from taking place.”\textsuperscript{12} The review concluded that the majority of the banks forming part of their review had not taken adequate measures to mitigate the risks of money laundering and terrorist financing in their trade finance business.

In October 2015, due to high volumes of trade and values of transactions in Singapore, the Monetary Authority of Singapore (MAS) published guidance on AML/Counter Financing of Terror (CFT) controls in trade finance and correspondent banking.\textsuperscript{13} The guidance highlighted 27 areas within risk assessments, due diligence, sanctions, correspondent banking, and trade-based money laundering concerns that required attention, and highlighted that overall AML and CFT controls for trade finance and correspondent banking were in scope for more robust controls.
In February 2016, The Hong Kong Association of Banks published a guidance paper with input from the Hong Kong Monetary Authority (HKMA) on Combating Trade-Based Money Laundering.14 The HKMA identified further need to implement effective measures and expected each accountable institution to give full consideration in the adoption of the best practices recommended by the paper, improving systems and processes where required to meet their regulatory obligations.

UNDERSTANDING GLOBAL TRADE

Prior to illustrating any framework for combating financial crime and money laundering, we must understand the context of contemporary global trade finance. In 2015, HSBC Global Trade and Receivable Finance accounted for more than USD $550 billion in documentary trade for its customers, making it the leading international trade bank.15 In 2016, the World Trade Organization (WTO) estimated that roughly 90% of the world’s trade was supported by some aspect of trade finance.16 According to a 2018 Bain & Company press release: Africa, Asia Pacific, and Latin America jointly account for 12.8% of global trade via trade finance documentation. These three markets have a larger perceived risk and uncertainty on payments. All large-scale volumes of trade require FI intermediation.17

It should further be noted that Asia Pacific on its own accounts for 6.2% of the above statistic, which does not include the Chinese Belts & Roads Initiative (BRI) aimed at strengthening China’s global position economically and strategically. It is understood that identified BRI economies may eventually account for one-third of global GDP and trade, and close to two-thirds of world population, some of which have inadequate infrastructure, weak AML controls, and other related gaps susceptible to TBML opportunities. According to Dane Chamorro, China has planned, developed, or obtained control of nine major ports, from East Asia across the Indian Ocean to Southeast Europe in order to leverage influence in commercial and trade interests.18

Global trade financial products normally consist of Core Trade Finance (Advance Payment, Open Account, Bills for Collection, and Letters of Credit), Guarantees, Receivable Finance (Factoring), Supply Chain finance and Commodity Structured trade finance.

The following briefly defines a few Global Trade and Receivable Finance (GTRF) products:

- **Core Trade**: Traditional trade products facilitated by FIs (as indicated above) by granting access to trade finance services. Letters of Credit provide the highest level of comfort to buyer and supplier. This process can be viewed below in *Figure 1*.
- **Guarantees and Standby Letters of Credit**: Permitting clients to pursue trade where risk mitigation specifics are provided or received.
- **Receivable Finance**: FIs facilitate exporters to obtain the proceeds of the sale immediately and collect the true receivable from the buyer on a later due date.
- **Supply Chain Finance**: Clients with a large portfolio provide expedited payments to suppliers.
- **Structured Trade Finance**: Products related to commodities, such as energy (petroleum and gas), metals (ferrous, concentrate, and base), and agriculture (coffee, cotton, cocoa, grains, etc).
The views and opinions expressed in this white paper are those of the author and do not reflect any official policy or position.

FIGURE 1: PROCESSING DOCUMENTARY CREDIT (CORE TRADE) AS PART OF GLOBAL TRADE

Citation

THE PSYCHOLOGY OF FRAUD AS A PREDICATE OFFENCE TO TBML

When there are large sums of wealth involved, such as in global trade, there are continuous risks associated with fraudsters and criminal organizations. Renowned criminologist Donald Cressey, who developed The Fraud Triangle, illustrated that individuals were more likely motivated to commit fraud when there existed a nexus of three elements: perceived pressure, perceived opportunity, and a manner or reason to rationalize the fraud.19

FIGURE 2: THE FRAUD TRIANGLE: PRESSURE, OPPORTUNITY, AND RATIONALIZATION

As viewed in Figure 2 above, the same theory is applicable today and followed by what is described as The Fraud Diamond, seen in Figure 3, now including “Capability,” which is largely interpreted as: “I can do it.”

FIGURE 3: THE FRAUD DIAMOND

The above theories highlight the nexus between fraud and TBML in the following ways:

- Criminal organizations may find themselves under pressure to create opportunities to either make money to finance other forms of criminality or layer the proceeds of their ill-gotten gains for the purposes of integrating the proceeds into formal economies. An example of the above is the Colombian Black Peso Money Exchange. Raymond Kelly, Commissioner of US Customs (1998–2001) once quoted, "The Black-Market Peso Exchange is perhaps the largest, most insidious money laundering system in the Western Hemisphere. It's the ultimate nexus between crime and commerce, using global trade to mask global money laundering."22

- Legitimate Organizations or individuals within those organizations, due to a restricted cash flow, may find the need to inflate liquidity. Due to the pressure, they may co-mingle legitimate and illegitimate trade receiving financing from FIs for non-existent trade.

- Opportunities may exist to commit the crime as a result of insufficient financial crime controls within an FI. There may further be inherent risks creating such opportunities in the absence of controls in relation to the structure of the trade product.

- Rationalization supported by pressure and opportunity adjusts the manner of thinking to contemplate that circumstance may dictate that it is worth taking the risk. This form of rationale may further be considered by those countries that are subjected to sanctions, highlighting that economic sanctions may lead to manipulation of invoices in trade finance.

- Capability related to perceived reality that one has the capability and all related opportunity to commit the fraud or engage in TBML and is prepared to accept the risks of the attempt.23 Such capabilities may further be enhanced by decisions to engage in alternative currencies to support false trade as a result of the US economic trade wars, that may not be subject to as much scrutiny across borders, for example from Russia to China (Ruble to Renminbi).
RISK CLASSIFICATION AND CHALLENGES IN TRADE FINANCE

In 2009, Reg Whitaker, author of “The Dark Side of Life: Globalisation and International Crime” stated that defining economic globalization is more complicated than the terminology “transnational corporations” and “international finance” would immediately suggest. More specifically, Whitaker was referring to that fact that there is a licit capitalist economy that is competing with a criminalized illicit economy. Essentially, the difference between the lawful and unlawful economies has consequences for the governance of the global economy. For example, in January 2019, the Malaysian government announced a prosecution case related to bribery, corruption, and money laundering pertaining to a BRI project to the amount of USD20B.

Traditionally, Trade and Receivable Finance is classified as both high risk and highly profitable, requiring the need for robust controls. Generally, the risks and challenges related to both the Lines of Business (LoB) and Compliance consist of the following:

- Multiple counterparties
- Multi-jurisdictional/cross-border
- Misrepresented transportation document in the form of Bills of Lading (BLs): presentation of invoices to various FIs for the same cargo with the intent to defraud and receive compensation for double or multiple financing
- Misrepresented invoices, stripping of information regarding the identity of the real buyer (fraud)
- Commodity and Structured Fraud Schemes: Possible cloned BLs, requiring human analysis
- Document centric and large volumes of data that poses risk if not well managed
- Large volumes of trade transactions
- Time-consuming, complex transactions could be used to layer the illicit movement
- Potential misrepresentation of financial statements by the client
- Segregation between review and investigations
- Manual paper-based processing
- The majority of transaction or monitoring surveillance systems used by most FIs dealing with commercial trade maintain the traditional rules-based software systems. It is challenging and costly to incorporate all the fields required for monitoring trade-based transactions.
- Pricing: over/under-invoicing market practice in some jurisdictions
- Difficulty in the detection of dual-use goods or technologies
- Intelligence sharing with law enforcement and other FIs due to potential data sharing or privacy restrictions
- Regulators or Central Banks may have minimal requirements on multi-banking or credit bureaus hindering the FIs’ ability to view financial credibility or distress of other companies, similar to the above mentioned on double financing of invoices and the use of multiple FIs for over lending with the intention of obtaining illicit financial gain
- Suppliers’ eligibility to supply the goods may not be verified by the FIs (medicine or controlled equipment may be accepted at face value)
- Potential co-mingling of legitimate and illegitimate trade
- Two-way trading

The views and opinions expressed in this white paper are those of the author and do not reflect any official policy or position.
- Companies registered in free zones or offshore financial havens requiring minimal UBO information
- Local road transport where the movement of goods cannot be validated as the actual transport, or transaction cannot be verified, allowing the exporter and importer to potentially misuse the Open Account facility by presenting fresh-air invoices, while there is no underlying movement of goods.

*Figure 4* below presents an example of how analytics and good investigative skills identified a TBML scheme consisting of social links between the buyers and suppliers. In this scheme, the offenders were recycling cash, cross-firing cheques, and performing inter-account transfers with the intent to abuse an FI trade finance product, where there was minimal movement of underlying goods, and all subsequently traced back to the same UBO.

**FIGURE 4: FINANCIAL CRIME RISK IDENTIFIED VIA SOCIAL LINKS IN A TBML SCHEME**

![Diagram](image)

**POSSIBLE HIGH-RISK INDICATORS OF TBML**

As discussed earlier, TBML is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions to legitimize their illicit origins. In this case—FIs that have effective AML compliance teams—high-risk indicators can be used to indicate possible risks of TBML. Red flags are not evidence of illegal activity but are only indicators that specific transactions “may deserve closer scrutiny.” The concerned investigator or analyst must consider certain factors when addressing possible red flags of TBML. Such factors include geographic locations, any history of trade fraud or criminal associations, normal transactions and activity of subjects, recognized value of the goods, and any presence of financial intelligence on any parties involved. Some of the significant high-risk indicators of TBML flags are listed as the following:

- Discrepancy in the description quality and quantity of the commodity documented on the BL and the invoice and the goods shipped
• Intentional under- and over-invoicing the value of the commodities on the Letters of Credit
• The weight of the shipment does not concur with the listed contents
• Shipment date and route does not match International Maritime Bureau (IMB) records
• Shipment between buyer and seller are in high-risk or sanctioned jurisdictions, or countries known to maintain inadequate AML standards, making use of front or shell companies
• Shipments involve delivery to free-zone or special economic-zone companies, which require minimal ownership information, and customs controls may merely be random
• Method of payment does not coincide with the normal business practice of involved parties
• Higher than 25% concentration risk between buyers and suppliers
• Goods do not fall within the business model of the exporter/importer or Line of Business (LoB)
• Round-tripping of funds
• Containerized shipments of auto-spare parts, electronics, and scrap metals to and from high-risk jurisdictions
• The exporter requests an unrelated third party to receive the payment
• The use of transport that cannot be verified (road transport in the Middle East is common typology used in a TBML scheme)
• Ultimate beneficial owners (UBO) of the buyers and sellers are found to be connected by means of investigative tool screening or social links. An example of this can be viewed in Figure 5 below. The diagram demonstrates the trade cycle over a period of one year and consists of the following:
  o The FI customer Tech Wise LLC availed import loans from the FI for all the transactions with the “Main Supplier.” The arrow marked in red for USD $10 million is the total of import loan funds flown out as repayment for goods purchased over the period. Loans are given with a due date (to be repaid by Tech Wise LLC).
  o Tech Wise LLC avails export finance from the FI, where the FI provides instant funds to Tech Wise LLC for the goods sold to buyers A, B, C, D, and E. The buyers repay the funds (green arrows) to the FIs’ nominated account on a future date, as stipulated by Tech Wise LLC.
  o As indicated in the diagram, Tech Wise LLC is directly linked to all the buyers via common ownership, the HR Manager being their main supplier. This conflict of interest is not disclosed to the FI.
  o Through the use of the trade product, Tech Wise was able to channel the funds, which originated from the buyers through the FIs, out to the supplier. The source of the funds from the buyers is unknown.
  o The funds that are credited to the supplier (via import loan) and the customer (via export finance) are directly from the FIs’ suspense account (with the trade bill/loan reference) and not from the direct account of the remitting party. This modus operandi aids distancing the identity of the source of the funds.
An example of recent trade-based financial crime was highlighted by EY in their publication entitled “Tricks of the Trade.” This publication mentioned the Indian Central Bureau of Investigation review of Baroda Bank transactions, where a trade-based money laundering scheme was uncovered. A total 59 account holders in the name of fake companies conducted almost USD $1 billion in illicit activity under the auspices of trading in rice and cashew shipments to partners in Hong Kong and the United Arab Emirates.

The following examples are typical findings in a TBML investigation:

- Majority suppliers managed by the same UBO; there is no declaration to the FI, intentionally concealing the supplier concentration. The suppliers are found to share the same telephone numbers, postal addresses, and common domains on their websites.

- Goods supplied differed from entity to entity, calling into question the ability to manage such a supply chain by one individual, where none of the other entities are financed by any FI within that jurisdiction.

- Goods supplied by the seller were controlled goods, yet the Trade Licence indicates the supplier as a “General Trader.”

- All transactions were conducted via local road transport, with no possibility to validate the movement of goods.

- Client regularly purchases goods from their own group company; however, this was not disclosed to the FI.

Another example of high-risk jurisdictions and the use of front shell companies is well illustrated in the recent “Troika Laundromat Scandal” of 2019. An investigative report by the Organised Crime and Corruption Reporting Project concluded that the now defunct Lithuanian-based Troika Dialog Investment Bank was used to transfer billions of dollars to offshore companies by using fictitious trade deals. The deals were invoiced variously as “food goods,” “metal goods,” and “auto parts.”
In addition, links between Sanctions and TBML in the form of misrepresented BLs have become common. For example, intentional false declarations are aimed at disguising the final destination or point of origin. This can be exemplified when, in early 2018, a dual Liberian-Korean registered ship was seized in Indonesia after it was found to have contravened the UN Security Council resolution 2397 (2017), which banned North Korea from exporting coal or conducting ship-to-ship transfer of goods. The investigation concluded that the misrepresented BL stated the country of origin as Russia while it was in fact North Korea. The use of applied analytics and software solutions will enhance the ability of FIs to identify and mitigate the above-mentioned examples of TBML and Sanctions Evasion, meeting their regulatory obligations.

It is noted and understood from all of the above examples, that irrespective of how regulators, law enforcement, and FIs enhance their TBML capabilities, organized crime continues to find innovative and sophisticated ways to defraud and launder money. This can be achieved through cyber technology, identification of “back doors” in FI “products and systems,” or gaps in the legal governance of the jurisdiction in question.

SOFTWARE SOLUTIONS AND APPLIED ANALYTICS

In today’s high-paced and globally connected economy, FIs have implemented strategies to enhance their share of international trade. It is also recognized that in this digital age, big data and AI offer both significant commercial value and the ability to streamline financial crime investigations. AI provides the ability to analyse data at pace, using various forms of algorithms and cognitive learning, assisting FIs to make faster decisions on trade transactions and risk mitigation, improving customer service, and managing more efficient and effective business.

A few of the emerging risks to FIs are listed below:

- Core Trade Product: Free of Payment. An example is a set of documents is sent to FI X for collection via FI Y. Upon receipt, a request is made to release the documents free of charge or against partial payment, mentioning that an advance payment was made by the importer. The intent is to possibly circumvent tax, regulatory requirements, or limit the FI visibility of the movement of underlying funds, meaning values do not align with invoices.
- Sanctions: Transhipment risks related to sanctioned countries (goods may be offloaded in a sanctioned country, not reach final destination); a transaction monitoring alert upon further scrutiny may highlight previously unidentified risks, requiring further look back at the client’s historic transactions.
- Cryptocurrency payments: ensuring that the right digitalized solutions are in place along with transaction monitoring while ensuring the Risk-Based Approach is able to mitigate any potential AML concerns on the origin and the source of funds for the payment of the goods.
- Continuous development of Free Zones: Free Trade Zones (FTZs) can offer important economic benefits for host countries and hosted companies, alike, but they can also contribute to trade in fake goods and other illicit activities.
- United Nations Economic Commission for Europe (UNECE): Advance Ruling used by governments provides an example of how the trade process in the Middle East is labour-intensive in terms of paperwork. The process allows for the prior declaration of classification, origin, valuation, and so forth to be applied to specific goods at the time of importing them.
The data collected could be obscured, along with insufficient document oversight, and port controls, as mentioned above, could result in higher risk exposure to FIs.32

- The unknowns of Mirror Trading money laundering schemes and how they could possibly translate into TBML, as criminals attempt to layer and integrate proceeds via FIs into economies. Both Deutsche Bank and Danske Bank were implicated in most recent emerging USD billion money laundering scandals.33

- In 2010, the IMB first highlighted BL fraud related to non-vessel owning common carriers (NVOCCs) and that FIs could unwittingly be processing fictitious BLs, where there are no supporting documents or that there was a misrepresentation of the shipments, a risk that is still prevalent today. As a result, the IMB has recently launched an initiative aimed to prevent the fraud risk.34

- Mitigating TBML and currency control evasion while pursuing growth opportunities affiliated with the BRI. Due to potential high volumes of data across the globe, a robust action plan is required.

The use of digital solutions aims to provide an efficient end-to-end trade finance platform. The digital solutions should be further supported by Intelligence-Led Financial Crime Risk Management (ILFCRM), such as those currently developed by HSBC, and the up-skilling of investigators will significantly improve both FI and regulator abilities to mitigate the risks of TBML.35 In December 2017, the head (Rob Grupetta) of the UK Financial Conduct Authority (FCA) explored, during his speech, “Using AI to keep criminal funds out the financial system,” how AI could possibly be used to mitigate money laundering, especially in the transaction monitoring space.36 Grupetta made an excellent point in relation to the implementation of AI, in that it was expected that the AI technology was embedded in a manner like any other, which included continuous testing, governance, and proper oversight.37 Between 2017–2019, there have been significant strides in both enhancing risk mitigation and the customer experience, leading to legitimate customers placing more faith and trust in the FIs and regulators, as well as law enforcement embracing the public-private partnership to address organized crime. One such stride is the implementation of Blockchain in trade finance.

Blockchain in trade finance has played a fundamental role in paving the future of trade transactions. In 2018, Reuters described Blockchain as a database that is shared across a network of computers containing records that, once added to the chain, is difficult to alter. The Blockchain network makes constant refining.38 In March 2018, HSBC launched a joint initiative with Quantexa (UK risk assessment firm) in the form of a Global Social Networks Analytics (GSNA) platform to mitigate the risks of human trafficking, money laundering, and terrorist financing.39 The GSNA platform gives a complete view of the bank’s clients, leveraging data in a dynamic manner and enhancing the investigators’ ability to identify unusual activity.40 This cutting-edge financial crime risk initiative was further recognized by CELENT (Fintech services firm), awarding HSBC with the Model Bank 2019 Risk Management Award for their initiative Fighting Financial Crime with Big Data Analysis:

“The Global Social Network Analytics platform offers HSBC a new and centralised approach to identify potential illicit activity. The platform provides investigators with the ability to access and analyse internal and external data from various sources across jurisdictions, presenting a contextual and comprehensive view of customer activities and relationships. This approach represents a significant step forward in the fight against financial crime.” 41

As part of the HSBC ILFCRM approach, the FI has set about hiring experts and developing new analytical techniques aimed to rapidly and efficiently work through large quantities of data that will both provide more accurate and timely information to law enforcement and regulators as well as
mitigate any actual or potential financial crime risk to the bank.\textsuperscript{42} In May 2018, HSBC and ING Bank completed the initial commercially viable trade finance via Blockchain for a shipment of soybeans from Argentina to Malaysia.\textsuperscript{43} The transaction conducted on a shared platform took less than 24 hours compared to the conventional of 5–10 days. As soon as the two parties have established a relationship, it is expected that there will be less risk mitigation from FIs, further enhancing the development of global supply chains and trade between parties based on trust. The use of Blockchain is aimed at minimizing the risks of fraud in Letters of Credit, which is a predicate offence of TBML, and enhancing customer experience by automating procedures.\textsuperscript{44}

The use of the above technology is a form of an introduced robust control identifying the client profile, as an FI sets out to explore new growth opportunities, balancing the needs of the LoB with needs of compliance. In October 2018, the HKMA launched eTradeConnect, the Blockchain trade finance solution that permits the financing of trade by digitizing the trade documents and automating the financing. The solution is aimed at reducing risks and improving efficiency and trust.\textsuperscript{45} In 2018, EY highlighted that any form of a trade financing monitoring solution would use advanced analytics to identify high-risk indicators, and, combined with compliance policy, would drive automated and improved decisions. The above approach is supported by ACAMS, in that FIs should create the mitigation that contains the following verticals:

- an alert-based pillar to monitor for unusual activity
- a second pillar’s ability to randomly choose transactions to provide quality assurance for potential illicit activity
- The third pillar puts a case management tool at the disposal of investigators, making them more precise
- The final pillar deals with reporting and providing out-of-the-box reports that can aid investigators and institutions alike in their trade-based monitoring of both importers and exporter.\textsuperscript{46}

Overall, this approach enhances the potential for FIs to grow their customer base in a safe and trusted environment, gives comfort to navigating a continuously evolving regulatory landscape, and sets the tone for the delivery of enhanced capabilities to mitigate financial crime risk.

RISK MANAGEMENT FRAMEWORK AND INTERNAL CONTROLS

It is noted from the examples of current regulatory guidance, TBML typologies, risks and challenges surrounding products and compliance, the psychology of fraud, and the use of AI, that this is the direction that FIs are moving to manage and mitigate the risks of criminality. For example, Crime Risk Management (CRM) “is an evolutionary and analytical process to assess whether organisational procedures, assets or individuals could become exposed to a potential threat; to identify the measures necessary to reduce any such risk; to mitigate the consequences of any hazard once realised; to evaluate the success or otherwise of the prescribed course of action; and to adapt appropriately.”\textsuperscript{47} It is understood that regulators and law enforcement may not have a consistent approach to mitigation as a result of local laws or data-sharing restrictions. There are quite a few known unknowns and risks yet to be mitigated surrounding controls, systems, and the various regulatory landscapes.

As a result, it is crucial that FIs take all extenuating circumstances into consideration while compiling the RMF, and that consideration is given to the implementation of the framework that caters for the
actual and potential risks. The ultimate goal is to provide an end-to-end capability to mitigate the risks of TBML. For the purposes of this paper, the RMF and OE is limited to the mitigation of financial crime controls of TBML. RMF is defined as the holistic management of the risks adopted by an FI to achieve its strategic goals pertaining to the mitigation of financial crime risk. The RMF requires certain objectives, scope, structure, and classification of risk in order meet the criteria of OE of AML and the wider financial crime risk controls.

A key objective of the RMF is “set the tone from the top,” promoting a strong compliance culture. Thomson Reuters describes the basics of the Compliance culture to consist of awareness, communication, education, effective technology, incentives, and incident reporting Case Management. It is argued that setting the tone from the top should go beyond incentives, as an FI RMF should comprise of certain values, such as dependability and accountability. Management in the FI, as well as its staff members, should also be able to separate right from wrong and promote a “speak up” culture to mitigate financial crime. The message communicated from the top is to be clear and understood in that all staff members have a role and responsibility in mitigating financial crime concerns.

Training is imperative to success and must cover the wider spectrum on how to mitigate TBML, not only analytics and software solutions. Since the unfortunate 9/11 attacks, emphasis has been placed on the significance of AML/CTF and filing of an SAR/STR; to an extent, the fundamentals of fraud and related crimes have been somewhat overlooked. The holistic approach including that of fraud in financial investigations has needed to be re-emphasised and included in more depth for financial investigators. It may be found that although money laundering is disguising the proceeds of crime, the predicate offence may not be clear in the SAR/STR. In reference to TBML, fraud is defined as a “knowledge misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.”

In 1996, Michael Porter defined OE to mean “performing similar activities better than rivals perform them. OE includes, but is not limited to, efficiency. It refers to any number of practices that allow a company to better utilize its inputs by, for example, reducing defects in products or developing better products faster. In contrast, strategic positioning means to perform different activities from rivals’ or performing similar activities in different ways.

FIs could consider the following when assessing OE:

- Are staff aware of the financial crime risks with the product (awareness and training, etc.)?
- Are staff aware how to escalate their concerns; in essence, how one raises an Unusual Activity Report (UAR)?
- Are staff aware what a good UAR contains, and that there needs to be a clear difference between what may be a financial crime concern versus something that relates to a business model gap where the client does not meet the terms and conditions of banking?
- Taking Compliance out of the equation, how does the LoB go about mitigating its risks and exercising control over those products and client base, and what is tested and when?
- How effective is the KYCC of the client?
- Does the recipient of the UAR timely meet its service delivery target of commencing an investigation?
- How effective are the warehouse visits?
- Request for Information (RFI): Is the RFI from the Compliance or Investigative function timely to the LoB or the client? Is it clear what is being asked to confirm, ensuring the client’s time is
CONCLUSION

Through the enhancement of technology, changes in the geographical landscape, and geopolitical events, the globalization of trade continues to evolve. It has created significant opportunities for financial growth and development of global infrastructure, while simultaneously creating opportunities for money launderers, terrorists, and those seeking to circumvent sanctions. FIs, in partnership with technology firms, are in the process of continuously revolutionizing technology to support trade transactions and the mitigation of financial crime risk. It is understood that criminals, irrespective of their rationalization, are motivated to search for loopholes to pursue defrauding avenues, whether it be exploiting those trade platforms by using cybercrime or alternative currencies or mechanisms to target gaps in products, processes, and systems in order to achieve their agenda, as it has been noted in recent scandals and vulnerabilities in FI controls. In numerous instances, fraud is identified as the primary predicate offence in TMLB and is also envisaged to play a pivotal role and preferred modus operandi, as economic sanctions continue to be imposed on targeted individuals and countries. The unknowns and anonymity of cryptocurrency pose risk to FIs, requiring an innovative investigative mindset to design robust controls to minimize risk exposure.

The key to an efficient RMF in support of mitigating TBML is to adopt a multi-disciplinary model that is designed to be accountable, practical, and as simple as possible to meet regulatory obligations. During the implementation of the model, it is foreseen that FIs will encounter both drivers and obstacles brought on by the regulatory landscape, demands on profit margins, customer experience, and mitigation of criminality. Irrespective of training, internal controls, data management, and the use of AI, the framework requires continuous monitoring and testing in support of the embedded OE in order to mitigate financial crime risk. The use of digital solutions, such as paperless cross-border transactions using Blockchain technology and machine learning (compliance technology), are on track to set the tone for the future of trade. This enhances safe growth of economies, supports finance investigations, and mitigates TBML. AI will be tested for its compatibility to data protection and regulatory requirements, along with its ability to mitigate financial crime risk. As AI continues to re-

The views and opinions expressed in this white paper are those of the author and do not reflect any official policy or position.
adjust its abilities, becoming cognitive to identifying new risks, it is understood that automation will not eliminate risk in its entirety, and should rather work hand-in-hand with human investigative analysis and decision making. It should not replace a financial crime investigator, nor the questioning discretion and judgement of the decision maker on how risk should be mitigated.
REFERENCES

Note to author: Each citation should include as much of the following information as possible, including electronic sources: author name, date of publication, title of document, and “Retrieved from: URL.” Also, make sure there is one space between each line, and that formatting is consistent.


