Opportunities for Advanced Analytics and Artificial Intelligence in Combating the Trade-Based Money Laundering and Financing of Terrorism

Savaş Külcü, CAMS
September 2019
Table of Contents

EXECUTIVE SUMMARY ....................2
TOPIC, GOAL, AND PURPOSE ..........4
PROBLEM DEFINITION ....................4
NATURE OF AND DIFFICULTIES IN TBML/TF RISKS ....................4
  Definition ................................4
  Categories ................................4
  Complexity ..............................5
  Challenges .............................7
ROLES OF FINANCIAL INSTITUTIONS IN COMBATING TBML/TF ....................7
  Role and Position in Combating TBML/TF ....................7
  Roles in Trade Intermediation ..........8
  Roles in Trade Finance ..................8
  Financial Crime Risk Management ....9
  Complexity of Managing the TBML/TF Risk ....................11
  Shortcomings of Combating the TBML/TF ....................12
ADVANCED ANALYTICS IN GENERAL ....................14
  Definition ....................14
  Requirements for Advanced Analytics 14
  Approaches in Advanced Analytics ....15
  Creation of Value through Advanced Analytics ....................15
ADVANCED ANALYTICS FOR COMBATING ML/TF ....................17
  Recent Regulatory Trends ..................17
  Perspectives for the Use of Advanced Analytics ....................18
  Methods Used in Advanced Analytics for Financial Institutions ....................20
ADVANCED ANALYTICS FOR COMBATING TBML/TF IN FINANCIAL INSTITUTIONS ....................22
  Data Considerations .....................22
  Detection of Price Anomalies ..........23
  Detection of Weight Anomalies ..........24
  Detection of Anomalies in the Profiling of Traded Goods for Countries ..........25
  Detection of Shipment and Shipment Route Anomalies .....................25
  Detection of Red Flag Anomalies ..........26
  Continuous Learning and Prediction Through Analytics ....................28
CONCLUSION AND FINAL THOUGHTS .....................29
NOTES .....................29
WORKS CITED .....................33
EXECUTIVE SUMMARY

The topic of this white paper is the opportunity to use advanced analytics and artificial intelligence in financial institutions (FIs) against trade-based money laundering and financing of terrorism (TBML/TF) by bringing new perspectives to the compliance community regarding its ability for using artificial intelligence and advanced analytics to increase the effectiveness of compliance programs for their financial institutions.

TBML/TF is the largest and most pervasive methodology on the one hand, and the least understood, recognized, and enforced on the other. The complexity and challenges of TBML/TF cause FIs to be exposed to great vulnerabilities, of which they are mostly not aware. Because of the role of banks as the responsible party for combating the financial crime defined in their compliance programs and their role in risk management, intermediation, and finance of trade, the effectiveness of combating TBML/TF is crucial from regulatory perspective, but also for economic and national security purposes.

Because of its nature, traditional combating mechanisms and human-centric control structures are not effective. According to overvalued imports and undervalued exports, the estimations of the sum of money laundered are enormous, whereas the numbers of suspicious transaction reports (STRs) are still low, which implies that the compliance programs of banks are not compatible with the risks stemming from TBML/TF.

Thanks to the enormous computation power, sophistication level, and availability of more data, it is no longer a dream to utilize advanced analytics and artificial intelligence not only for TBML/TF in particular, but also for money laundering and financing of terrorism (ML/TF) in general. The use of advanced analytics offers new perspectives and can create value, still yet to be tapped.

Recent regulatory developments encourage FIs to invest in and use advanced analytics and artificial intelligence in combating ML/TF, an area that has not been sufficiently commercialized and widely standardized. The existing monitoring and screening systems for combating ML/TF are mainly designed with knowledge-based systems. Even a proven system whose focus is on combating TBML/TF does not exist in the market place. This implies that there is great economic potential for this area as well. This potential can be better exploited if the existing regulatory encouragements will be continued and intensified, and if the cost of compliance, both directly and indirectly in terms of investments and penalties, will be appropriate.

After having stated the topic, goal, and purpose of this white paper, in the first section the problem definition is made by questioning the effectiveness of detecting and predicting the schemes of TBML/TF with existing structures and capabilities of compliance programs of financial institutions.

In the second section, the nature of and difficulties in TBML/TF risks are presented in terms of definition, categories, complexity, and challenges of TBML/TF.

In the third section, the roles of financial institutions in combating TBML/TF are depicted in trade intermediation and trade finance, and financial crime risk management practices are discussed. Additional complexities of managing TBML/TF risks and the shortcomings of combating TBML/TF are also described.

In the fourth section, advanced analytics is introduced generally by providing a definition, stating the requirements for advanced analytics, presenting the approaches in advanced analytics, and mentioning how value through advanced analytics can be created.

In the fifth section, advanced analytics for combating ML/TF is presented, starting with recent regulatory trends, continuing with perspectives for the use of advanced analytics, and finalizing with methods used in advanced analytics for financial institutions.

In the sixth section, opportunities for advanced analytics for combating TBML/TF in financial institutions are presented. Data considerations are mentioned initially, and then potential use cases are exhibited. Continuous learning and
prediction through analytics topics are also stressed in this section.

In the last section, a conclusion is presented, and final thoughts are said.

There are many use cases for advanced analytics and artificial intelligence in combating TBML/TF that are right to the point, meaningful, and feasible. These can be implemented either before the fact, as in the pre-transaction phase; through the fact, as in the in-progress phase, as a preventive measure to avoid any involvement in such a crime; or after the fact, as in the post-transaction phase, as a detective measure. Nevertheless, these use cases include detection of price anomalies, detection of weight anomalies, detection of anomalies in the profiling of traded goods for countries, detection of shipment and shipment route anomalies, and detection of red flag anomalies. There are potentially many more use cases, the presentation of them, however, are beyond the scope of this work.

The vision of using advanced analytics and artificial intelligence in the compliance world, and even in combating ML/TF, is not new. However, the vision of using advanced analytics and artificial intelligence in combating TBML/TF is innovative and inspiring. I hope that the compliance community will share my vision and contribute to the realization of this vision with me.

Finally, I would like to thank Mr. Dennis M. Lormel, my mentor for this white paper, who supported, encouraged, and inspired me to work on this topic.
**TOPIC, GOAL, AND PURPOSE**

The topic of this white paper is the opportunity to use advanced analytics and artificial intelligence in financial institutions against trade-based money laundering and financing of terrorism.

The goal or objective of this white paper is to bring forward new perspectives to the compliance community regarding its ability for using artificial intelligence and advanced analytics as an opportunity to gain effectiveness and efficiency in combating trade-based money laundering and financing of terrorism.

In order to understand the potential contribution of and opportunities with the use of artificial intelligence and advanced analytics, the complexity of trade-based money laundering and the financing of terrorism will be presented; challenges and complexities associated with existing detection and prevention approaches will be exhibited; and the effectiveness of financial institutions will be questioned.

The potential for the effectiveness and efficiency of financial institutions could only be realized to the extent that suspicion is raised for undetected schemes and potential illicit business that are commingled with legitimate business, so that criminals and associates are weeded out from customers who have legitimate business and licit activities.

**PROBLEM DEFINITION**

It has been indicated by the Financial Action Task Force (FATF) that TBML is one of the methods used for money laundering (1) and is deemed to be one of the complex forms of money laundering. (2)

As key players in the intermediation and finance of international trade, and as responsible parties for the compliance with the requirements set forth by the Bank Secrecy Act (BSA), banks should take responsible and prudent steps to combat money laundering and terrorist financing, and minimize their vulnerability to the risks associated with such activities. (3)

However, given the complex nature of the risk, the shortcomings experienced by financial institutions, and the critical role of them in combating TBML/TF, the solutions designed and used by financial institutions that are not compatible with the nature of the risk are still ineffective and contrary to the widespread and increased use of advanced analytics and artificial intelligence in various fields of banking and financial services. Therefore, the benefits of using advanced analytics and artificial intelligence, in particular for financial crimes risk management, have not been fully utilized and have not been discussed thoroughly by risk professionals.

Thus, the definition of the problem questions whether the existing structures and capabilities of compliance programs of financial institutions are effective enough to detect and predict the schemes of TBML/TF without advanced analytics and artificial intelligence. Also questioned is whether the potential use cases for engaging advanced analytics and artificial intelligence have been seriously considered and utilized.

**NATURE OF AND DIFFICULTIES IN TBML/TF RISKS**

**Definition**

TBML was defined by the FATF in 2006 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 origins.” (4) The FATF paper on best practices (2008) broadened the definition and stated, “TBML and terrorist financing (TBML/TF) referring [refers] to the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illegal origin or finance their activities,” and included illegal activities such as terrorist financing to be covered within the scope of TBML. (5)

TBML and value transfer in all its forms outlined below, can be regarded as the largest and most pervasive methodology on the one hand, and the least understood, recognized, and enforced on the other, (6) and requires more than a mere definition of what it is and how it works.

**Categories**

It is possible to categorize TBML/TF in various ways, mainly based on the methodologies used
or the goods traded that are subject to laundering. Due to its nature, there is hardly any unique and common categorization, however the following categorization may highlight how multifaceted TBML/TF is and how difficult it is to figure out.

In principle, the main category is the transfer of value and laundering of funds by trade through:

- misrepresentation of pricing (by overstating or understating the price, value is transferred between exporter and importer);
- invoice fraud (by issuing multiple invoices or altering the true nature of items on the invoice, other than price, quantity, or quality);
- nonexistence of shipment (by using deceptive techniques, appearing as if a genuine shipment exists, a phantom shipment);
- misrepresentation of quality of goods in a shipment (by trading inferior goods of poor quality but documenting the transaction as if of high quality or vice versa);
- misrepresentation of quantity of goods in a shipment (by trading less goods but documenting the transaction as if more goods are being traded or vice versa); and/or
- deliberate obfuscation of the type of goods (by causing a different type of good to appear on the documentation other than the good being traded).

In the above mentioned category, there is collusion between the seller and the buyer in which the intended outcome of a deceptive technique is to obtain a benefit in excess of an arm’s length transaction.\(^7\)

Another category involves laundered funds being used in the conduct of legitimate trade. In this category, trade as a transfer of value is not used to launder money, but rather legitimate trade is being victimized by using illegitimate funds through:

- the export or import of goods by legitimate business, which is being financed by illegal money,\(^8\) mainly through third-party settlements or bulk cash payments (either by the possible lack of business ethics of engaged parties, use of complicit merchants or straw buyers, or due to insufficient know your trade partner requirements); and/or
- counter-valuation or balancing the books of hawaladaars in underground financial systems,\(^9\) known as alternative remittance systems or informal fund transfer systems\(^10\) (by settling accounts of hawaladaars among each other, by bundling over a period of time after a series of transactions in both directions in the form of import-export clearing,\(^11\) and not necessarily by misrepresenting the price, quantity, or quality of goods traded).

The trade in the above-mentioned category could be legitimate; however, the source of funds used to finance the transaction or settle the accounts is generated through crime.

Another category of TBML/TF is the trade of illicit merchandise, particularly in the form of contraband, narcotics, arms, nuclear material, or any good subject to licensing or restrictions. Any proceeds generated from illegal trade can apply based on the intention and capability of the parties involved, including the financing of terrorism,\(^12\) or continuing and promoting the committing of crime. This form of TBML/TF trade is not only a source of proceeds, but it may also be a method for the transfer of value, depending on the conditions.

The final category involves the trade of dual-use goods, which are products and technologies whose primary use is for civilian purposes but may also be for military applications.\(^13\) Contrary to the previous category, in which trade of illegal goods or goods that are subject to special scrutiny and treatment, trade of dual-use goods are legal. However, due to its nature, intermediation, settlement, or finance of trading such goods necessitates special and due care,\(^14\) especially against the financing of terrorism and sanctions management.

**Complexity**

As outlined above, TBML/TF is one of the least understood methods of financial crime. The following aspects will contribute to the understanding of its complexity.

One of the aspects of complexity is the mixed use of TBML/TF methodologies with other ML/TF typologies and methodologies. When focusing only, for instance, on
misrepresentation of price, quality, or quantity of goods traded, it is highly likely that in most cases a combined use of structured cash transactions, funnel accounts, cross-border wire transfers, shell or front companies, and hawala-type underground financial systems will help figure out the scheme and avoid myopia.\(^{(15)}\)

Another aspect is the convergence and diversification of terrorist organizations and criminals. Terrorists and criminals, who have different interests and intentions, and whose typologies and patterns differ, find increasingly common ground of mutual benefit. When intersection of these two different profiles maximize mutual benefit, convergence will be expected. Whereas, whenever increase of maturity in organization and sophistication takes place, diversification will be expected.\(^{(16)}\) Thus, when it comes to TBML/TF profiles, patterns and motivation of both sides, as well as the effect of convergence and diversification, should be considered. Thus, it is to be discussed whether the case is a laundering of money, financing of terrorism, or maybe both.

The cross-border nature of international trade poses an additional challenge to the complexity of TBML/TF. The intermingling of the trade sector with the finance sector, together with the customs offices in cross-border transactions, creates difficulties in cross-border information exchange and provides opportunities for criminals to take advantage of differences in legal systems of various jurisdictions.\(^{(17)}\) This aspect is more facilitating for laundering when shell or front companies from less cooperating, sensitive, or high-risk jurisdictions are used, or when shipments to or from free-trade zones, which have poor transparency, take place.

Variation of standards across jurisdictions brings additional complexity. Many jurisdictions do not have a common formatting or categorization for trade data collection and suspicious activity reporting. This does not enable collection, dissemination, and analyzing of information available, and understanding of the scope and extent of the threat posed by TBML/TF.\(^{(18)}\) Organizations and institutions, including FIUs, law enforcement agencies, regulators, and customs offices, have different standards of data governance and protocols for data exchange, which impedes effective processing of data to information and from information to intelligence. The variation in data governance and exchange has wide-reaching negative implications across the jurisdictions as well.\(^{(19)}\)

Variation of standards is not limited only to data but extends to legal directive, training, and competence of law enforcement agencies across the jurisdictions as well.\(^{(20)}\) In some cases, differing jurisdictional standards may cause less stringent controls,\(^{(21)}\) and because of the lack of awareness due to risks associated with TBML/TF, it is possible that in some jurisdictions detection of schemes by a bank and raising the right level of alert by a FIU will be less effective.

Long supply-and-value chain in trade is another factor that increases the complexity. Because international trade is realized by many actors, including manufacturer, trader, exporter, importer, consigner, consignee, financier, shipper, insurer, freight forwarder, financial intermediater, customs broker, etc., negligence or incapability of any actor along the chain may facilitate the laundering activity and distract from deterring and detecting laundering.\(^{(22)}\)

Another factor is the use of free-trade zones and transshipment. Because of their tax regulations, relaxed oversight, and lack of transparency, free-trade zones can be facilitating from a TBML/TF perspective. Potential misuse of free-trade zones creates additional vulnerabilities when goods like cigarettes, alcohol, electronics, which can be converted easily into cash as a transfer of value, are being traded.\(^{(23)}\) Transshipment could create an environment more prone to TBML/TF because of the possible extra points of entry for laundering and lack of transparency inherent in the origins of shipment. Information deficits in the shipping and transshipment industry obscure the details of shipment, which are critical for TBML/TF purposes. When containers are transshipped through free-trade zones and held in storage, it is likely that before being shipped to the next destination reprocessing of the goods in containers takes place in the form of repacking, breaking bulk, subdividing, relabeling, or consolidation, which helps disguise the track of goods and creates additional vulnerability for monitoring.\(^{(24)}\)
Engagement of multiple FIs and multiple roles of FIs bring additional complexity. Depending on the type of transaction, a bank provides different services, mainly financing, intermediation, risk mitigation, or settlement. Depending on the structure of payment and the availability of documentary credit, a bank assumes different roles. For instance, in a documentary credit, a bank can be a transerring, advising, conforming, negotiating, discounting, reimbursing, remitting, or nominated bank. Another transaction may require engagement of more than two banks in which, for instance, a second advising bank (with or without confirmation or with a back-to-back letter of credit) can be engaged, or a bank issuing a slave letter of credit can be present. Moreover, similar, recurrent, or connected trade transactions can be broken up and dispatched to different banks by the launderers to disguise the real source and nature of a transaction. Thus, difference in services and roles, as well as expectations of and requirements for them, in terms of know your customer (KYC) and financial crime controls, make TBML/TF even more complex.

As a result, these factors contribute to the complexity of TBML/TF, which leads to difficulty in understanding the true nature of risk and countering with appropriate measures.

Challenges

In addition to the complexity of TBML/TF, there are various challenges which complicate the deterrence and detection.

One of the challenges is that there are financial crimes similar in apperance but different in nature. Our aim is not to give the full list of crimes or explain their true nature, but rather to raise awareness in order to help distinguish TBML/TF from other crimes. Some of the methods used, such as overpricing or underpricing, may occur in cases where strict capital controls exist in a jurisdiction, and capital flight is schemed by means of trade. Use of abusive transfer pricing is another crime through which corporates try to avoid taxation with fictitious valuation techniques. Invoice fraud is another crime that is motivated by earning of export incentives. With carousel fraud and ficticious export or import, refunding of value-added tax is the motivation for using techniques similar to TBML/TF.

Sheer volume of transactions and increased amount of trade volume present additional challenges, which create a high level of noise regarding the level of legitimate trade, namely genuine trade, and mask criminal activity. Also, front companies are used to mask the true nature of trade, and legitimate funds are commingled with illicit proceeds in order to disguise the source of funds.

Use of countertrade in terms of barter, counter purchase, or buy back further complicates the combating of TBML/TF. If publicly available or reasonably predictable, a fair price of a good can be judged regarding the existence of any risk through misrepresentation of price. However, when it comes to countertrade, there is the problem of exchange ratio which with a good is traded vis-a-vis for another good. The problem of determination of a fair-exchange ratio is exacerbated when a partial payment is considered in the exchange. The use of barter trade is also favored and used, like the method of laundering, due to the intransparent nature of countertrade, as well as the existence of limited foreign currency and the motivation for the evasion of taxation or reporting.

Another challenge is that, mainly due to privacy concerns, there is a lack of effective data exchange between countries, law enforcement agencies, and public and private sectors. Shortcomings in the exchange of data between countries are partially overcome by the establishment of trade transparency units. However, not every country has been integrated as a partner to the United States, nor have countries other than the United States devised an effective system similar to it.

ROLES OF FINANCIAL INSTITUTIONS IN COMBATING TBML/TF

Role and Position in Combating TBML/TF

Banks are responsible for having a compliance program in which risk assessment, know your customer (KYC), customer due diligence, financial crime risk controls, and suspicious
activity reporting (SAR) are required. Trade finance related specific requirements are set forth in each jurisdiction, either as a separate chapter\(^{36}\) or mentioned in a broad sense.

Trade can be broken into the following steps, some of which may be overlapping:
1. Arrangement to trade goods
2. Financial steps to facilitate the trade
3. Movement of goods
4. Reconciliation or settlement of financial accounts\(^{37}\)

The second step refers to the trade finance, whereas the last step refers to the intermediation of banks. The second and fourth steps jointly refer to the risk mitigation of banks on behalf of trade partners. Therefore, risks associated with TBML/TF should be aligned with these steps, and expectations of banks in relation to TBML/TF risks should be commensurate with the role, position, and capability of banks along the long supply–and–value chain stated above.

As banks deal with documents, and are not involved in transportation, delivery, exchange of goods, or performance to which the documents may relate, the biggest challenge of banks is to define the right basis for degree of scrutiny to be applied and for understanding an unusual activity.\(^{38}\) Considering the fact that international trade:
- involves the movement of goods, documents, payments, and data, and
- is mainly conducted around 80 percent in open account terms,
the banks suffer from the lack of transparency, when open account terms are being applied in which data necessary to identify and detect an unusual wire transfer is not available.\(^{39}\)

Thus, as a matter of fact, for nondocumentary transactions, banks are not provided with the supporting documentation, reducing the information available to review and assess the risk of being a victim of TBML/TF. The situation is more desperate when netting of transactions between a buyer and a seller takes place, and there is no chance of tracing back a transfer to a specific trade transaction. Unless a hit due to a matched name of any party to a transfer for sanctions purposes coincidently occurs, the chance of identifying a transfer as risky is almost zero.\(^{40}\)

### Roles in Trade Intermediation

The role of intermediation of a bank and the management of financial crime risks vary, depending on the existence of a customer relationship with other banks and the parties involved in any transaction or structure, and the nature of relationships between banks.

Correspondent banking is a form of customer relationship, briefly defined as the provision of current account and related services of a bank to another bank for execution of third-party payments and trade finance, or for a bank’s own purposes, cash and liquidity management, short-term borrowing, and investment needs. Because of its ongoing and repetitive nature, and the payment processing of customers of a respondent bank, it is likely that KYC and due diligence deficiencies of a respondent bank could expose a correspondent bank to and contaminate it with potential risks.\(^{41}\)

Therefore, not only should the risks associated with a respondent bank be reviewed and assessed, but also customer transactions of a respondent bank should be monitored closely as in the role of a remitting bank.

Contrary to correspondent banking, in a noncustomer relationship, a bank does not have a payment account through which third-party payments of the noncustomer bank are being processed, but rather, because of intermediation, only bills for collections are being presented or collected as in the role of an importer’s bank. Because the relationship allows only for a SWIFT relationship management account, and only MT 400 message series for documentary collections can be used, identification of risk for TBML/TF on behalf of importer’s bank is limited and the lack of full payment process is apparent.\(^{41}\)

Therefore, KYC and due diligence measures of the exporter’s bank are decisive, and reliance on the controls of the importer’s bank would be ineffective.

### Roles in Trade Finance

The role of a bank in terms of trade finance, and the management of financial crime risks vary, depending on the type of financing, the structure of the transaction, a bank’s side to a transaction
as exporter’s or importer’s bank, and the expectation from the bank.

Type of financing could be in the form of documentary credit, documentary bills for collection, demand guarantees, standby letters of credit, trade loans, bank payment obligations, or even open account terms as payable finance and receivable discounts. Each type of financing has specific financial crime control requirements and challenges. When it is about, as expected in trade finance, the control of documents to identify red flags and unreasonable fact patterns, for instance, banks have chances to examine documents thoroughly in a documentary credit, demand guarantees, or standby letters of credit. Whereas, in documentary bills for collection, because of absence of any specific terms and conditions against which to check them, a detailed examination of documents attached to a bill is unproductive. More troubling is the situation if a bank is involved in a bank payment obligation in which financing is being executed only through data matching, and specifically requested documentation can be asked for to conduct an examination only after and as part of sanctions monitoring, or post-transaction AML monitoring, when something triggers other than the trade finance transaction in question.

Besides, the role of a bank is decisive according to the side a bank assumes on a transaction, either as exporter’s or importer’s bank, and according to the expectations of an exporter’s or importer’s side on a transaction from a bank, either in the form of risk mitigation, provision of financing, or settlement. As usual in a documentary credit, for instance, the importer’s bank is assumed to be the issuing bank and to conduct specific controls for a trade finance transaction. However, if the bank is assumed to be the exporter’s bank, the extent and scope of controls vary according to, among others, the structure of the deal, the issuance of the credit, and the relationship with the issuing bank. Whether advising, transferring, confirming, negotiating, discounting, or making payment on behalf of the importer’s bank or reimbursing bank, the role of an exporter’s bank changes with varying degrees of risks and controls, which also increases the complexity of combating TBML/TF.

Financial Crime Risk Management

As outlined above, the roles and positions of banks vary, including responsibilities and necessities in terms of controls, reviews, and assessments. Broadly speaking, these can be separated into three phases according to the steps a trade transaction should basically follow, which will be described briefly below.

Before the fact, as in the pre-transaction phase, customers should be assessed based on their TBML/TF risks, which is called the risk-based approach. For this to happen, a more focused KYC process is to be fulfilled to assess, among other things, business model and size. Types, volumes and prices of goods, countries traded with, trading partners, terms of trade, mode of payments, and routines that are relevant for KYC should also be collected. Based on the internal risk assessment and KYC information gathered, a decision can be made as to whether enhanced due diligence should be applied to a customer in general, or specific transactions and transfers of a customer in particular.

This is the phase in which the inexhaustible and never-ending lists and categorization of red flags from the literature of TBML/TF should be reviewed to find out which red flag categorization, red-flag definition, and threshold for these red flags could be selected, calculated, mixed up with each other, and calibrated in order to identify anomalies. This process is to be designed in such a manner that the risk assessment and KYC information are taken into consideration to best reflect the customer risks of a portfolio.

The aim of this paper is not to present a categorization or a full list and definition of red flags, but rather to give an insight of why and how they can be designed, used, and made beneficial. Given the vast and abundant literature on red flags for the sake of simplicity, a brief categorization of red flags could be broken down according to:

- customer (e.g., risky small business engaging in a transaction incompatible with its business size and strategy);
- transaction (e.g., transaction involving an unusual intermediary);
- structure of deal (e.g., structure of the deal between exporter and importer appearing
Opportunities for Advanced Analytics and Artificial Intelligence in Combating the Trade-Based Money Laundering and Financing of Terrorism

unnecessarily complex and designed to obscure the true nature of business;

- goods (e.g., vulnerable goods traded that are not expected to be traded between countries in which trading parties are residing in);
- jurisdiction (e.g., one of the trading parties located near the border of a risky jurisdiction);
- shipment (e.g., shipment not economically realistic in terms of size of goods traded and container occupied);
- documentation (e.g., significant discrepancies between the description of goods on the bill of lading and actual goods shipped); and
- payment (e.g., unusually favorable payment terms, such as payment substantially far above or below expected market price or lump-sum cash payment).

Red flags can be configured according to the availability and quality of data, the degree of detail and scrutiny needed, and the results of the risk assessment.

Through the facts of the in-progress phase, after having built up a control environment and taken a series of risk-management measures, any application of a customer for a trade transaction to a bank will be handled. Given the results of the risk assessment, KYC information, requirements for enhanced due diligence, and availability of and relevance with pre-transaction red flags, controls are completed—each from a different perspective, as the nature of each application may differ from the other.

The application of a customer is reviewed and assessed, given the existing fact pattern and additional red flags associated with customer requests throughout the process, as by carrying out the authentication of documentation and validation of information and data fields. If not satisfied with the outcomes of process controls, completion of the application will be held for further process or release of payment for the settlement of an account.

After the fact, as in the post-transaction phase, various activities are carried out, some of which are listed below:

- Review of customer documentation and data compared and updated in order to be more precise in due diligence
- Conduct of trend analysis in terms of trade transactions and trade-related transfers
- Conduct of anomaly analysis regarding the post-transaction red flags and scenarios for account activity
- Conduct of post-event analysis for the detection of reasonability based on customer activity
- Review and process of letters from law enforcement agencies in terms of any necessity for further action

As the final step, the results of post-transaction analysis results are assessed in order to find out any amendments that are beneficial or necessary to update the risk assessment and customer acceptance policy. Customer relationship is also considered as to whether the existing relationship should be terminated, confined, subjected to enhanced due diligence, or determined to be as satisfactorily compliant.
Complexity of Managing the TBML/TF Risk

The role of FIs in the long supply-and-value chain poses a great deal of complexity for FIs regarding the detection of suspicion in TBML/TF. As indicated above, several parties, including manufacturer, trader, exporter, importer, consigner, consignee, financier, shipper, insurer, freight forwarder, financial intermediary, customs broker, etc., are involved in a trade transaction. Thus, the whole chain of a trade deal in which a bank is typically engaged—either as providing with documentary credit, settling an account, or conducting a payment—is not fully visible for a bank. The lack of reliable statement of customers, data, and documents regarding the activities of other parties along the chain complicates detection of the true nature of a transaction.

Varying degree and limited involvement of FIs are other factors increasing the complexity. As mentioned regarding the roles and positions of the FIs, banks assume various roles depending on the availability of documentary credit, engagement in and intermediation of other financial institutions, existence of customer relationship, and robustness of compliance controls. The data available at the discretion of any FI to raise a suspicion differs. Given that international trade is mainly being conducted around 80 percent in open account terms, and the launderers’ approach is to break up a transaction into several steps and dispatch them to different banks, FIs are not usually well provided with relevant data to assess the risk of TBML/TF.

Use of informal value and fund transfer systems is another factor creating additional complexity. When some form of these systems is being engaged for a trade transaction, FIs normally lose track of necessary transaction logs, and the nontransparent nature of these sytems with bundling and netting off several transactions makes it even more complex for FIs to understand the true nature of a trade transaction, even when hawaladars are customers of a FI.

Use of shell and front companies could bring more complexity due to their nontransparent ownership and control structure, particularly when a company had been onboarded as a legitimate business, but during the course of relationship, because of intermingling of illicit funds with legitimate funds, the risk of TBML/TF could not be easily detected. Some criminals are so professional in disguising the source of funds and using deceptive techniques that reasonability of business cannot be detected with comfort by using traditional KYC controls and reviews. This is the case if, for instance:

- goods are traded, whose expected market price is not publicly available, or due to customization, a fair market price cannot be judged;
- vulnerable goods are traded mainly in the form of consumer goods, textiles, garments, electronic goods, leather, precious metals, jewelry and diamonds, commodities, arts, or luxury items, which have high turnover and values, and some of which have high taxes or duties; or
- the FI is not the only bank that intermediates international trade activities of a company.

As a result, it could be almost impossible for a bank to decide on the suspicion of a front company, unless other fact patterns and red flags support the reasoning.

Complex structures and products in trade and trade finance cause additional complexity. When criminals leverage complex structures to disguise the true nature of a transaction, or they prefer complex and sometimes innovative trade and trade finance products, rather than conventional products with full documentation, especially in documentary credits, tracking the logs and collecting the data necessary for raising suspicion could be troublesome.

**Shortcomings of Combating the TBML/TF**

Given the complexities and challenges of the TBML/TF risks in general and the additional complexities of FIs in particular, there are various shortcomings that FIs have to confront in combating TBML/TF, one of which is the limited automation and document-based operations. Paper-based processing of documentary credit transactions for FIs does not allow them to capture the data printed on specific data fields, which are invaluable for designing the fact pattern and feeding the right data into the right red flag, through which minimizing the dependency for manual work can be attained and risk of detection can be reduced. Currently, transaction monitoring systems do not support automation and pattern recognition fully; however, they are still under development. (47)

Lack of appropriate and qualified data leads to shortcomings, particularly due to the manual and document-based nature and limited automation of trade processes. Another factor amplifying this problem is the need for structured external data sources, such as shipment tracking, customer identification, beneficial ownership data, or market price data in order to decide on the reasonability of a transaction. Integrating them into the internal customer, transaction, and payment data to configure meaningful determination of red flags is another challenge. (48) Furthermore, internal data quality deficiencies coupled with nonavailability of or missing external data complicate the detection process, because authentication of existing documents and data with external data sources could also be hindered. (49)

Verification of trade-related pricing data is another shortcoming causing FIs to develop and maintain effective financial crime risk controls against TBML/TF. Because of their role as financial intermediary and provision of risk mitigation, and not being and acting like a businessman, FIs are not capable of making meaningful interpretations and determinations about the legitimacy of unit price of any goods traded by their customers, even though a robust due diligence has been conducted. In addition to the lack of relevant business information about unit prices, characteristics of business relationships between sellers and buyers, which affect the terms of delivery and sale, credit facility of sellers, volume discounting, and product customization, cause the unit prices of similar products to vary substantially. Even for publicly traded goods with similar nature and characteristics, which enable FIs to make meaningful comparisons, current prices may not reflect the effective sales price. (50) That is why commercial services are being offered by third-party service providers, allowing FIs to make inquiries about the generally accepted price of a particular commodity. (51)

Lack of qualified staff with TBML/TF knowledge also causes shortcoming. In relation to trade intermediation and trade finance, bank staff can be roughly categorized as relationship managers and trade processing, trade financing, compliance, and audit staff. Trade intermediation and trade finance are generally complex and niche areas in which long years of experience are required to fill related posts, so most banks find it difficult to recruit competent staff for these posts. Each category of staff has specific qualifications and has different training requirements with respect to ML/TF in general and TBML/TF in particular. Because of limited
Opportunities for Advanced Analytics and Artificial Intelligence in Combating the Trade-Based Money Laundering and Financing of Terrorism

automation and a document-based approach of handling customer applications, judgement of staff is critical for detecting anomalies in trade intermediation and trade finance.\(^{52}\)

In addition, problems associated with qualification and number of staff are multiplied when escalation of a suspicion from the first line of defense to the second and third lines of defense happens, and staff for compliance and audit is not capable of understanding the true nature of risk raised to them, due to a competency gap between different roles within an organization. Thus, all levels and lines with different roles should have a common understanding, which is not widely observed.

Dispersion of qualified staff across the lines of defense is another factor contributing to shortcomings. As indicated above, there are different roles required, some of which are dispersed across the bank with different focus and qualification. It is not necessarily true that every qualified and experienced relationship manager, trade-processing, or trade-finance staff really have in-depth knowledge about TBML/TF. Thus, generally the staff from the first line of defense has extensive knowledge about customer, product, and process, but lacks the TBML/TF knowledge, whereas the compliance staff in the second line of defense is more oriented on TBML/TF but has deficiencies in customer, product, and process. It is a rare phenomenon that the full skill and competency set for combating the TBML/TF, which also necessitates in-depth customer, product, and process knowledge, is dispersed across the organization. As a matter of fact, the higher the deficiency is in the first line of defense on the disadvantage of TBML/TF, the higher will be the susceptibility and vulnerability of FIs.

Lack of focus for combating TBML/TF due to various other compliance requirements for trade also causes a shortcoming. Intermediation or financing the trade-based transactions requires additional compliance controls, reviews, and assessments other than TBML/TF. Depending on the jurisdiction, the relationship with the customer, and the structure of the trade deal, international trade may be subject to additional compliance requirements, including these requirements:

- Sanctions
- Tax
- Customs
- Foreign exchange controls
- ICC (International Chamber of Commerce)
- Licensing requirements compliance
- Credit policy and regulations compliance (if the transaction is being financed)
- Incentive regulations compliance (if the deal targets a benefit for export or import incentive)

Thus, given that TBML/TF is more challenging and demanding than any other ML/TF methodologies, and given that other compliance requirements listed above require relatively less effort, staff of FIs tends to have less focus for and spends less time on TBML/TF compliance controls.
ADVANCED ANALYTICS IN GENERAL

Definition

Advanced analytics is a collection of related techniques and tool types, including predictive analytics, data mining, statistical analysis, complex SQL (structured query language, a standardized programming language used to manage relational databases and perform various operations on the data), data visualization, artificial intelligence, and natural language processing.\(^{(53)}\)

It is:

- more than just numbers to find out and report observed correlations and statistical distributions;
- knowledge and results centric, and focuses on the process of discovery of actionable knowledge; and
- tools agnostic, and uses any computation or visualization tools from statistics, computer science, machine learning, and operational research to describe and recognize patterns, seek and validate causal relationships and trends, and predict and optimize outcomes.\(^{(54)}\)

Analytical modeling tools are used for predicting outcomes of:

- likelihood of certain occurrence or events;
- grouping of people or entities;
- values of transactions; and
- meaning and attributes of anything other than above.\(^{(55)}\)

Requirements for Advanced Analytics

To use advanced analytics, the availability and quality of data with which the models will be built upon are of critical importance. Poor or inadequate data is one of the biggest challenges for analytics; however, in many instances, quality of data is never perfect. It is likely that there are significant missing, duplicated, outdated data or entry errors in data that could challenge the quality of model results. Analytical models can still be generated \(^{(56)}\) if validation performance remains acceptable after:

- data imputation in which through replacing the missing data by average, mean of the nearest values or a prespecified value; and
- elimination of data with questionable quality through cleansing and augmentation of data-quality problems.
However, because of the necessity for using big data to build up analytical models, apart from availability and quality, there are still data concerns as in the form of:

- volume (terabytes, records, transactions, tables, files, etc.);
- velocity (batch, near time, real time, streams, etc.); and
- variety (structured, unstructured, semistructured, etc.).

Other data concerns should also be taken into account. For instance, the following are being used more and more in big data analytics:\(^{(57)}\)

- unstructured data (text, human language, audio, video, etc.) that is converted into structured data through text mining and text analytics; and
- semistructured data (XML: Extensible Markup Language, a standard used as a flexible way to create information formats and electronically share data via public Internet and corporate networks; or RSS feeds: Really Simple Syndication, a way to easily distribute a list of headlines, update notices, and content used by computer programs, which organizes the headlines and notices for easy reading, etc.) that is driven up by increased use of industry standards such as SWIFT.

Analytics professionals are using tools on the path to AI, including machine learning by leveraging algorithms or mathematical models that learn from data to gain insights that were previously out of reach. The existing analytics solutions facilitate machine learning with multilayered, fully optimized algorithms that enable computer models to generate insights from complex and unstructured data without explicit directives. Deep learning is a branch of machine learning that uses artificial neural networks that learn from experience by using deep graphs with multiple layers to form models that can infer insights from new data.\(^{(58)}\)

**Approaches in Advanced Analytics**

Depending on the maturity, scale, and complexity of advanced analytics, as well as opportunities to be generated from them, there are various approaches:

- In *descriptive analytics*, the main goal is to find out what has happened for a human-centric decision and action. The main outcome is defined as hindsight. Using dashboards allows learning from past behaviors without root-cause analysis.

- In *diagnostic analytics*, the main goal is to find out what has happened and why it has happened for a human-centric decision and action. The main outcome is defined as insight. Dashboards help drill down, using hierarchies or doing comparisons to find reasons or factors.

- In *predictive analytics*, the main goal is to find out what will happen, why it will happen, and when it will happen for a less human and more machine-centric decision and action. The main outcome is defined as foresight. It utilizes various statistical and machine-learning algorithms to provide recommendations as an estimate of a possible future outcome.

- In *prescriptive analytics*, the main goal is to find out what should be done to make it happen with machine-centric decision support and automation systems. The main outcome is defined as simulation-driven analysis and decision making. It utilizes recommendations for the best course of action to choose to bypass or eliminate future issues.

- In *cognitive analytics*, the main goal is to simulate computerized human thought with almost full machine-centric decision and action. The main outcome is defined as the self-learning and completely automated action. It is inspired by how the human brain processes information, draws conclusions, and codifies experience into learning.\(^{(59)}\)

**Creation of Value through Advanced Analytics**

There are various opportunities that can benefit an organization by using advanced analytics, some of which will be outlined below:

- Know your data is the key for success in designing and using advanced analytics. In terms of availability, quality, volume, velocity, and variety, an organization discovers the requirements for collection, transformation, and maintenance of data, and invests in data management, if decisions and actions should be based on analytics.

- Qualified and timely intelligence presents another opportunity to realize and act upon an incidence or event, which could necessitate prompt reaction, not only for effects, but also for root causes. Investigators
and compliance staff will be presented with improved and enhanced ways of viewing large masses of data in a manageable format.

- More case leads can be generated and processed by discovering the hidden relationships, detecting the unknown, unknowable, and sometimes unique events, and reducing the amount of time required to sort through dirty data.
- Increased precision can also be attained by delineating the most powerful leads as well as by dealing with incomplete and imprecise information more effectively through processing information and helping draw conclusions out of it that are otherwise impractical or inconclusive.
- Recognition of behavioral changes is another opportunity advanced analytics can offer. Sometimes the difference between expected behavior and unexpected behavior would not be easy to detect. Rather than just data, advanced analytics can show trends and attributes in a multidimensional format with distinguishing colors, shapes, and layers in a nutshell. An investigator can see anomalies in the customer’s accounts.
- Detection of behavioral anomalies is a major challenge when compliance professionals search for a needle in a haystack. Not every unexpected behavior could necessarily be an indication of a suspicious case. Spending time and effort would be generally paramount when massive dimensionality of customers X accounts X products X geography X time should be analyzed (X refers to times). Advanced analytics could increase the likelihood that an unexpected behavior could be a strong indication of a suspicion.
- Detection of networks is one of the biggest challenges a compliance professional can encounter. Not every criminal launderer his or her own funds alone, but does this mostly through structuring and layering the funds, and engaging various unconnected launderers in a scheme. Thus, the detection of links across the parties of criminals, launderers, and middlemen can be very cumbersome and mostly incomplete. However, thanks to link analysis and clustering potential, suspects can be grouped by communities that behave similarly or by their complementary outcomes of behavior.
- Recognition of group behavior could be another challenge. Detection of a network sometimes does not help to understand the roles of actors within the networks. Depending on the power relationship of actors in a network, direction, frequency, and amount of funds transferred, etc., it is possible to recognize and understand how a network structure operates in a scheme. Thus, useful insight could be attained for filing a suspicious transaction report.
- Use of advanced analytics keeps compliance professionals updated about how customers interact, what kind of new typologies are being used, what the main trends are, which vulnerabilities of an organization are being exploited, etc. Therefore, it is a great opportunity for continuous learning.
- Another opportunity could be the holistic and integrated approach an organization can gain by using advanced analytics. Thanks to the big data processing capacity, huge amounts of data being processed, and intelligent methods being used, the human-centric, disaggregated, and error-prone way of managing financial crime risks across the organization can be handled in a more connected and integrated fashion.
- Optimization of resources could be another opportunity for an organization if advanced analytics are used. Once data-driven and data-intensive ways of managing financial crime risks are being given priority, many subjective, judgemental, and sometimes wrong decisions about allocation of resources in terms of capacity, distribution among different teams, and focus areas could be reassessed and right-sized.
- Usually, prioritization of cases is being handled according to the time an alert is being generated. Mostly due to time pressure and cost management, compliance professionals have to deal with backlogs and miss important cases that deserve more dedicated resources for investigation. With the help of advanced analytics, a more intelligent prioritization of cases can be attained, and misallocation of resources can be minimized.
ADVANCED ANALYTICS FOR COMBATING ML/TF

Recent Regulatory Trends

In the Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, December 3, 2018, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration, and the Office of the Comptroller of the Currency jointly encouraged banks to consider, evaluate, and, where appropriate, responsibly implement innovative approaches. In the statement, it was mentioned that banks are becoming increasingly sophisticated in their approaches to identify suspicious activity by building or enhancing innovative internal financial intelligence units, which are devoted to identify complex and strategic illicit finance. It was said that banks also experiment with artificial intelligence applicable to their compliance programs, which can strengthen compliance approaches as well as enhance transaction monitoring systems.

The agencies welcome these types of innovative approaches to protect the financial system against illicit financial activity, and it has been argued that these types of innovative approaches can maximize utilization of banks’ compliance resources. It was stated that pilot programs that expose gaps in a compliance program will not necessarily result in supervisory action, with respect to that program, when banks test or implement artificial intelligence–based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes. In this respect, the agencies encourage the use of innovative approaches and technologies, including advanced analytics and particularly the use of artificial intelligence for strengthening the compliance programs of banks.\(^{60}\)

As the next step, the Financial Crimes Enforcement Network (FinCEN) announced the FinCEN Innovation Hours Program to better shape and inform its ongoing engagement with AML/CFT innovators. The program will provide financial technology (FinTech) and regulatory technology (RegTech) companies and financial institutions the opportunity to present their new and emerging innovative products and services. The FinCEN Innovation Initiative is a new initiative designed to foster a better understanding of the opportunities and challenges of AML-related innovation in the financial services sector. FinCEN recognizes that private sector innovation, either by new ways of using existing tools or by adopting new financial (FinTech), regulatory (RegTech), or other technologies, has the potential to enhance
financial institutions’ BSA/AML compliance programs.(61)

As a foundation for the new vision briefly mentioned above, the Under Secretary of the Department of the Treasury, Mrs. Sigal Mandelker, stated that the agency is open to innovative ideas from the private sector as to how they can strategically promote such information sharing within industry, and the agency is encouraged by innovations in financial institutions to combat financial crime. In recent years, financial institutions have improved their ability to identify customers and monitor transactions by using new technologies that rely on artificial intelligence and machine learning.(62)

The Executive Order on Maintaining American Leadership in Artificial Intelligence explicitly states that artificial intelligence (AI) promises to drive growth of the U.S. economy and enhance its economic and national security. Agencies of the government should pursue strategic objectives in promoting and protecting American advancements in artificial intelligence, including the promotion of sustained investment in research and development (R&D) in collaboration with industry, academia, international partners and allies, and other non-federal entities to generate technological breakthroughs in artificial intelligence and related technologies, and to rapidly transition those breakthroughs into capabilities that contribute to economic and national security.

Therefore, investment in artificial intelligence is being regarded as one of the strategic objectives for economic interests as well as for national security issues. Financial crime, laundering of illicit funds, and terrorist financing can be regarded as, among other things, the biggest threats to national and financial security. In this perspective, investments in innovative technologies for combating financial crime, particularly using artificial intelligence, is of paramount importance.(63)

In this subsection, a sample of perspective will be briefly presented regarding the use of advanced analytics in combating the ML/TF in order to demonstrate that, given the sophistication reached in computation and data processing, there is yet unexploited but enormous potential not in ML/TF but also in TBML/TF. Most of the literature about the use of advanced analytics in combating financial crime lacks detail and is presented from the perspective of governmental agencies or from their staff, rather than from FIs or compliance staff. Thus, private sector’s perspectives and use cases have not been thoroughly represented and reflected. However, this does not hinder compliance, analytics, and technology professionals from thinking about and being inspired by the existing use cases for advanced analytics in order to design, test, and use innovative approaches in their own domains.

The FinCen Artificial Intelligence System (FAIS) is used to process and analyze all reports received. FAIS uses data that has been extracted from BSA reports as transactions. Transactions associated with the same person are transformed to a new set of data, called subject, while transactions associated with the same bank account are used to create a data element for the account. Grouping of transactions into subjects and accounts is completed based on the information in each transaction—e.g., name, address, Social Security number, etc.—in order to find an acceptable level of similarity for aligning transactions with an assumed same subject.

Elements of data in the form of transactions, subjects, and accounts are further analyzed in a knowledge-based system to find out whether and evaluate to what extent they are suspicious. Based on the indicators apparently associated with the transactions and additional indicators calculated, a numeric score is assigned for suspiciousness that is based on rules which contribute positive or negative evidence as to whether the transaction-subject-account is deemed to be suspicious.

On the basis of these scores and many more criteria that are relevant for further investigation, the selection process is initiated and accomplished with link analysis, in which identification of networks of financial activities
Opportunities for Advanced Analytics and Artificial Intelligence in Combating the Trade-Based Money Laundering and Financing of Terrorism

is aimed to help distinguish between legitimate and illegitimate business activity.\(^{(64)}\)

This is a typical representation of descriptive analytics, in which data mining and clustering are being conducted with a knowledge-based systems approach. It has been extended to integrate with the analysis of the potential associates by using link analysis. However, it has limitations of a typical expert system, whose performance is heavily affected by the level of expertise in design capability of the rules and the architecture of the system. Depending on the data and the level of expertise, it is possible to build up a capability to identify and learn from the unknown patterns with this kind of artificial intelligence.

Another example could be the use of Harmonized Commodity Description and Coding System (HS), which is known as a harmonized system, developed by the World Customs Organization, and comprises about 5,000 commodity groups identified by common six-digit code. It helps in achieving uniform classification of goods traded and is applied by more than 200 countries for customs tariffs purposes. For the sake of comparative analysis and identification of anomalies related to trade of goods, it has been used for monitoring especially governments and customs because almost 98 percent of the merchandise is being classified in terms of a harmonized system.\(^{(65)}\)

The use of a HS is also mentioned as a means of analyzing the financial and trade data for identifying trade anomalies. A technique is being suggested to compare domestic and foreign import/export data to detect discrepancies in the harmonized system, country of origin, importer/exporter, unit price, commodity, activity by time period, port of import/export, etc.\(^{(66)}\)

An analysis based on the U.S. merchandise trade database, using the Harmonized Commodity Description and Coding System, revealed that there is plenty of room for identifying unit price and weight anomalies by using advanced analytics. The International Price Profiling System (IPPS) is used to produce statistical price filters to assist in detecting abnormally priced goods, and evaluates the risk characteristics of prices related to trade transactions. It evaluates a price based on different filters for the world as a whole and for the particular country under assessment by using edge percentiles, mean and standard deviation of prices. The statistical filters are calculated from 12 months of international trade transaction data from the sources of the U.S. Department of Commerce. Based on the outcomes generated, a risk index is calculated, and a high index score with a negative value is regarded as a suspicion for money being moved out of the country under investigation; whereas, a high index score with a positive value is assumed to be a reflection of a suspicion for money being moved into the country under investigation. The magnitude of the index reflects the likelihood that a price discrepancy of undervaluation or overvaluation could take place.\(^{(67)}\)

This is a typical example of descriptive analytics using data mining for extensive amounts of data to detect edge outcomes of prices of goods traded. Even though this may be an indication of suspicion, a further investigation is required as to whether it is a false alert in terms of operational error in data, indication of customs fraud, or a transfer pricing case. The level of precision depends on the expertise of specialists who design the rules and thresholds. However, this analysis is a good example of how trade data can be utilized in TBML/TF.

The analysis of international trade data is another example of how advanced analytics can be used. Trade Transparency Units (TTU) have been established. They examine the trade between countries by comparing the exports of country A with the corresponding imports of country B, and identifying any discrepancies between the data provided as it could be an indication of trade or customs fraud, or TBML/TF. In this context both domestic and foreign trade data are fed into a database and analyzed, using a tool called Data Analysis and Research for Trade Transparency (DARTT). DARTT is a computer system designed to analyze anomalies in international trade data, a tool which allows investigators and analysts to generate leads and support investigations.\(^{(68)}\)

The idea of analyzing trade data comes from collecting and combining the existing trade
data, at the discretion of each individual government, on a single database, and integrating the data into a single platform for further investigation. How the DARTT system operates and processes the data is an issue that is beyond the scope of this work. What is critical here is the importance of data availability and sustainability, rather than the architecture of the system or the rules used to generate the leads associated with TBML/TF.

Methods Used in Advanced Analytics for Financial Institutions

Banks conduct various screening activities and documentary reviews that help identify anomalies in individual transactions, but they do not enable banks to identify unusual trends and patterns before a transaction is completed or a transfer is released. By comparing with historical transactions, many monitoring systems can flag some of them for further investigation based on predefined rules and thresholds. Most of these systems are used after the fact in a post-transaction phase, either in batch mode operated with monitoring and alert-generating tools or as reviews on a periodic basis comprising the whole transactions.

Thus, the capability of banks to detect suspicious transactions before the fact in the pre-transaction phase and through the fact in-progress is mainly limited to sanction screening, which works online, generates a match, and blocks a transfer or an application with preloaded lists. This means that TBML/TF systems do not prevent the transaction to proceed but rather help in recognizing the abnormality afterwards.

Knowledge-based systems are computer programs that process the data in such a way that emulates human experts. Different from the algorithms, the knowledge embedded within the system is separate from the reasoning methods used to operate on the knowledge. The path of evidence and facts used to reach a specific conclusion is shown, and the inferences made are displayed and expressed in terms of rules, which connect the data to the conclusion either directly or through generating intermediate conclusions used by other rules within the system indirectly. The collection of rules is the knowledge base, which emulates the expert and is the input to an algorithm called inference engine, which uses data and knowledge base to come to a conclusion, either suspicious or not.

The critical issue is the reasoning embedded in the knowledge base, which is mostly acquired by domain experts or less frequently by analyzing the cases (believing their outcomes are correct) with data mining or through knowledge discovery. This so-called knowledge engineering may use relevant heuristics of experts (a technique or approach to problem solving, learning, or discovery that employs a practical method not guaranteed to be optimal or perfect, but sufficient for the immediate goals) and their common sense to reach out a rule. However, in addition to that, once diverse and multifaceted techniques of statistics, machine learning, and data visualization are employed, it could also be possible to identify as yet unknown and unknowable patterns.

Other than knowledge-based systems, there are a bunch of advanced analytical methods, some of which will be briefly presented, which could be beneficial to compliance professionals and investigators.

Logistic regression is a method of data mining that helps to solve problems especially for categorical variables, e.g., variables described as black or white answers. This method can be useful to analyze the data for classes of interest, and outcomes of it can be exhibited in graphs so that it is possible to visually grasp the common characteristics of subsets of variables. Graphs of trends in data can be displayed in multiple formats, which expediate the user to categorize the data.

Cluster analysis is most applicable when a grouping into few categories with similar attributes is required out of a substantial amount of data. It could be useful as it helps to generate leads in categories which could make sense, for instance, geographically or chronologically. It could be of great importance to apply it when aiming at an isolation of statistically significant relationships that is otherwise not apparent at first glance, and may not be even after extensive analysis.
Inductive algorithms are algorithms that generate decision trees based on the historical outcomes, and then produce rules from historical occurrences of the data out of these trees. Inductive algorithms create classifications of data by organizing them into categories and matching them with the decision-tree patterns so as to reach mutually exclusive alternatives of relationships, which could be an indication of unique paths that launderers could follow.\(^{(70)}\)

Neural networks utilize computers to mimic how a human brain operates in learning a structure. Such a network accepts inputs, conducts an array and sequence of operations in the data, and produces outcomes. Neural networks are a set of interconnected elements called nodes, and each node has a weight, indicating the strength of the influence of the value of one node on the value of another. Through adjusting the weights on each connection, these networks can be made to produce nearly any output on a given set of inputs. That is to say, in a set of data in which each observation contains an input in the form of a transaction or a transfer, and a known output as suspicious or not, the network can be trained to recognize the patterns in the data if they exist. By learning from examples of inputs and desired outputs, and by storing this knowledge in a neural network, simultaneous processing of continuous and categorical variables and handling the nonlinear and colinear data are made to be possible.\(^{(70)}\)(\(^{(71)}\)

Fuzzy logic is a method which allows users to make use of incomplete and imprecise information, process the information as if they are nearly complete and precise, and derive conclusions out of this information, which could otherwise not be meaningful. This helps users to spend less time and effort to work on data, lacking a standardization or elements, which is necessary to combine and connect other data bases or data elements.\(^{(70)}\).

Genetic algorithms are based on evolutionary rules (e.g., reproduction, mutation) used to solve a variety of optimization tasks. It can be used to depict more precisely the most powerful leads which could imply a suspicious case by saving time and effort to recognize and handle it.\(^{(70)}\)

Visualization is another method used to explore relationships between variables by applying colours and interactive graphics. Rather than constructing models, visualization enables users to examine data in order to apply their own personal expert knowledge and to benefit from their common sense by helping them recognize patterns in the data, which a model of machine learning has not yet duplicated.\(^{(71)}\)

As outlined above, the systems can be broken down mainly into knowledge-based systems and other advanced analytical techniques, which do not rely on the expert but generate learning and, based on this learning, create leads that could point to a suspicion. It has been argued that knowledge-based systems insufficiently train behavioral models, tend to give more false positive alerts, and fail to identify logical links between behaviors. It has also been stated that these systems do not effectively identify overlap and conflict of rules within the system. On the contrary, it has been argued that models generated by advanced analytics combine attributes into nonlinear behavior-based neural networks, which help to reduce false positives by assigning a score to unusual activity.\(^{(72)}\)

Whatever the argumentation and the reasoning for the application of models designed with advanced analytics, and whether they are credible enough to prove themselves as the new generation of models, there is a search for more and more advanced approaches. Such approaches could outweigh the disadvantages of knowledge-based systems and, thanks to the giant computation power, sophistication level, and availability of more data, benefit from the value created through methods of advanced analytics.
ADVANCED ANALYTICS FOR COMBATING TBML/TF IN FINANCIAL INSTITUTIONS

The use of advanced analytics and artificial intelligence could bring new perspectives and dimensions for combating ML/TF. As outlined above, TBML/TF has various complexities and many challenges in its nature as well as in the management of financial crime risks that result. TBML/TF has implicitly additional complexities and challenges in FIs, which usually expose FIs to very serious vulnerabilities, many of which they are unaware, and accordingly do not take such risks and threats as seriously as they should. This is, in particular, due to the fact that the existence of TBML/TF deficiencies in compliance programs and the ineffective combating of TBML/TF cannot be directly and easily addressed by and linked with the FIs’ involvement in and intermediation of trade transactions with ML/TF motives and patterns. Mostly, FIs could defend their stance by emphasizing the very complex and challenging nature of TBML/TF as well as the lack of monitoring and detection technologies that enable them to equip with necessary means against these risks.

Nevertheless, these perspectives and dimensions associated with advanced analytics and artificial intelligence could offer various opportunities for financial institutions and regulatory technology companies, which could design, develop, and offer innovative technologies. Availability and commercialization of these new technologies offered by Regtech companies could bring a new dynamism to the compliance technologies market landscape. The initiatives started by the FinCEN as well as the joint encouragements expressed by the agencies of the US government could hopefully bring a leap and dynamism in this context.

Data Considerations

As briefly outlined above, one thing is of essential importance: That is the data. As long as the problems of data availability and quality are resolved, there is a great potential for applying these new technologies. High sophistication of computing and large capacity for processing huge amounts of data can no longer be treated as problems. Depending on the use case to be worked on, data volume, velocity, and variety are also to be considered.

Another aspect is the digitalization of the documents and paper-based processing of trade
transactions. For the retrieval of the data, which is already available on documents in different formats but not digitalized yet to be processed, optical character recognition (OCR) technology can be used to capture and collect relevant data fields. These can vary from specific data fields, such as goods traded, unit price, port of discharge, or landing, etc., to names of persons who might be sanctioned in OFAC lists.

Another point is that the extracted data from the documents, through the use of OCR technology or the data which is already available in databases, can be incomplete or imprecise to further process. As mentioned briefly above, fuzzy logic methods can be used in filling the missing elements of the data fields. Fuzzy logic works on the concept of deciding the output on the basis of assumptions, and is regarded as an approach to computing based on degrees of truth. Thus, rather than not utilizing incomplete or imprecise data, which might be of critical value, a predicted value can be used.

As a final point, for the extraction of information from printed, scanned, or text files that are not organized and structured, capabilities of text analytics could offer new perspectives. With the help of text analytics, data elements scattered across the organization in an unstructured format can be transformed into a structured format, which can be further processed for databases that might be relevant for checking and monitoring.

In the following sub-section a sample of opportunities for the use of advanced analytics and artificial intelligence will be presented in brief, outcomes of which are decisive for identifying the suspicion in TBML/TF.

Detection of Price Anomalies

As mentioned in the categories of methods used for TBML/TF, mispricing is one of the methods used to move funds in or out of the country. Because scrutiny for obvious overpricing or underpricing of goods is requested for the FIs, the problem is how to identify the mispricing as functioning for intermediation, finance and risk mitigation, but not acting as a field expert to judge on right pricing. Besides, even if this happens, how is the level of obviousness defined?

One solution could be designing a price reasonability checking system, which operates before the fact as in the pre-transaction phase for each single transaction, and a price reasonability monitoring system, which operates after the fact, as in the post-transaction phase for periodic reviews of transactions processed. The requirements for these systems are to design a workflow and define data sets necessary for identifying the reasonability.

As indicated above, a Harmonized Commodity Description and Coding System enables FIs to describe and categorize the goods traded. The prices of the goods traded, based on the harmonized system codes as the unique identifier, can be retrieved from the databases of the U.S. Census Bureau’s U.S.A. Trade Online portal. FIs can gather export and import data regarding countries, prices, weights, and ports from which an analysis of reasonability as the “reference set” can be based. The price data and harmonized system code of each single customer are collected as the “control point” during the application process.

The workflow requires the comparison of every single “control point” with the relevant corresponding “reference set,” matching them through the harmonized system code and the time period in which the price of traded goods can still be valid in terms of market conformity. Goods could also be further categorized based on their vulnerability (e.g., electronic consumer goods, gold, tobacco, etc.) to be used in TBML/TF, or based on the countries in which trading partners are located (e.g., risky jurisdictions, sanctioned jurisdictions, countries with which a preferential trade agreement has been signed, etc.), or based on the routes of shipment (e.g., free trade zones, trade hubs, etc.) through which the traded goods are transported.

The reasonability checking can be configured so that outliers in terms of price imply a suspicious trade transaction. This can be done through the inter-quartile range price analysis in which, according to transfer pricing regulations, exceeding the upper inter-quartile import prices of imported goods and being less than the lower inter-quartile export prices of exported goods can be regarded as outliers. Alternatively, depending on the vulnerability of goods,
countries of origin, trading party, routes of shipment, or any element deemed to be a point of concern, the range for anomaly can be customized and varied, rather than fixing it to be as a quartile. The determination of the degree of variance, as outlined above, and the dynamics of change in variance can be configured with and decided by an artificial intelligence component as to whether the transaction in question deviates from the “reference set,” and if so, whether the deviation implies a suspicion or not.

Based on the decision as to the suspicion, an application for a trade transaction can be rejected, accepted, or flagged for further investigation in the pre-transaction phase. The rejected, accepted, and flagged ones, with varying weights of importance, can be used to make the artificial component learn from these transactions. In the post-transaction phase, all transactions are being reviewed and assessed periodically in terms of price reasonability, and outcomes of this process can be used to teach the artificial intelligence component.

Detection of Weight Anomalies

As mentioned in the subsection for price anomalies, in addition to the price, there is a requirement for scrutiny of weight anomalies as well. The same problem about the existence and level of reasonability is still valid for weight. For the sake of simplicity and avoidance of duplication, similar aspects and dimensions with the detection of price anomalies will be omitted.

In addition to and similar with the workflow mentioned for a price reasonability checking system and a price reasonability monitoring system, compatible checking and monitoring systems can be designed as well. The focus point for this subsection is designing a capacity reasonability checking system before the transaction being processed, and capacity reasonability monitoring system after the transactions are being completed.

The key point here is the determination of capacity for a customer under due diligence. This can be defined for manufacturers, traders, and manufacturing traders differently, and the necessary information should be collected during the know-your-customer (KYC) process. As banks usually collect and verify various information about the operating and business models of their customers, information used to calculate and predict for capacity is not explicitly mentioned. However, for managing the TBML/TF risk of customers, collection of information for capacity in terms of weight of sales is of critical importance. It should be considered that this information could be collected periodically:

- Capacity to produce in units for a period of time (e.g., annually)
- Weight of a unit product, including package
- Size of a unit product, including package
- Number of units sold/to be sold to international markets
- Percent of international sales

Containerization is the practice of carrying goods in containers of uniform shape and size for shipping. Anything can be stored in a container for the transport of manufactured goods. The use of containers in international trade is widely accepted; 90 percent of the world trade is carried through container ships. Standard ISO shipping containers of 8 feet have an 8 ft (2.43 m) length, 7.6 ft (2.26 m) height, and 7 ft (2 m) width of outside dimension, have a maximum gross weight of 13,243 lbs (6,000 kg), and tare weight of 2,100 lbs (950 kg). Thus, depending on the type and size of standard container, the sale for a customer can be calculated based on weight and size of a container.

According to the data to be collected in the KYC process, it is possible to calculate the number of containers a customer can fill for international trade in a period of time, which would be assumed as the “reference set.” As this reference capacity is calculated on the customer basis and is at the customer’s discretion to distribute his or her international trade transactions among the banks, this “reference set” should be adjusted to a single bank in question. Based on the level of customer relationship and the proxies generated for predicting the wallet share of international trade, which is a domain for customer analytics, it is possible to calculate expected trade transactions and capacity in terms of containers for the bank in question.
Once the customer applies for a trade transaction, the weight of a shipment in terms of containers as the “control point” can be calculated and journalized in a separate ledger, and the balance of the ledger is booked on a cumulative basis. If the sum of the applications for trade transactions exceed the “reference set,” an alert can be generated for enhanced due diligence. Various advanced analytics methods can be utilized for the design of capacity reasonability checking system; however, for checking and monitoring the transactions of same or similar goods traded for the same customer in time series, or multiple customers with similar goods across the section, artificial intelligence can be used to decide on the anomaly of unit weights.

Detection of Anomalies in the Profiling of Traded Goods for Countries

According to the law of economics, some countries specialize in goods and services for which they have relative advantages in terms of factors of production. This is due to the use of natural resources, human resources, technology used, or promixity to markets that are better than anyone else’s. Therefore, not every country specializes in all goods, but rather in those goods for which they have either less cost, high profit margin, better know-how, or abundant resources.

This phenomenon is reflected in the trade data between countries as well. Thus, each country has a trading profile similar to some other countries, but different than the others. Based on these facts and public databases, such as the U.S. Census Bureau’s U.S.A. Trade Online portal, by using cluster analysis and inductive algorithms, trading profiles of countries can be generated. Profiles of countries in terms of goods exported and imported according to type, weight, price, value, port, and time will tell the bank how the global market acts. For a more-focused approach, a bank may confine itself with profiling of the home country and countries trading with the home country in order to have the first “reference set.”

However, this does not necessarily mean that the customers of a bank trade goods exactly similarly to the home country. Due to business model, local market conditions, credit policies or risk appetite, the trade profiling of the customers of a bank could substantially differ from the profiling of the home country. Therefore, a profiling for the customer portfolio should also be prepared in terms of goods exported and imported according to type, weight, price, value, port, and time. This will be the second “reference set.”

In the next step, the variances between these two reference sets should be calculated so as to recognize if and to what extent the customers of a bank differ from the home country. The magnitude and direction of variances, simultaneous combination of multiple variances, and change in variances might be decisive in the identification of an anomaly, because the decision for anomaly will be given after an application for a trade transaction as the “control point” is compared with both “reference sets” and calculated with varying weights.

After having completed the profiling and comparison with the “reference sets,” the decision trees as to whether any trade transaction could be identified as suspicious can be designed. This will be the core for the profile reasonability checking system, which operates before the fact as in the pre-transaction phase for each single transaction, and a profile reasonability monitoring system, which operates after the fact as in the post-transaction phase for periodic reviews of transactions processed. The decision trees will be updated based on the decisions as to whether the transactions are rejected, accepted, or flagged for further investigation.

Detection of Shipment and Shipment Route Anomalies

Every trade transaction must have:
- shipment vehicle (e.g., rail, truck, air, vessel, etc.);
- shipment points (e.g., port of lading, port of discharge, port of trans-shipment, etc.);
- shipment route (e.g., exporting country, transit countries, importing country, etc.); and
- shipment type (e.g., individual, collective, transportation chain, etc.).
The shipment types in International Commercial Terms (e.g., Free on Board, Cost and Freight, etc.) have nothing to do with the types stated above. Individual shipment is similar to full container loads (FCLs) as the exclusive shipment; individual shipment means:
- one or more deliveries;
- one point of departure;
- one destination; and
- one mode of transport.

Conversely, collective shipment is similar to less-than-full container loads (LCLs) as partial shipment; collective shipment means:
- one or more deliveries;
- several points of departure;
- several destinations; and
- one mode of transport.

In transportation chain, however, there are multiple modes of transportation; for instance, the container is first loaded to a rail, then carried by a vessel, and delivered by a truck to the final destination.

There is various shipment information to be considered in a trade transaction, some of which has been mentioned above. However, for the definition of an anomaly, the following criteria as examples should also be considered:
- For a shipment, points to visit or pass through should be as few as possible.
- Duration of a shipment should be as short as possible.
- Modes of shipment should be as few as possible.
- Number of vehicles used should be as few as possible.

A complexity score can be calculated based on the criteria stated above by assigning higher scores to a shipment with more points, more modes, more vehicles, and longer duration, and vice versa for lower scores. The higher the complexity score a shipment has, the higher the likelihood will be that a shipment implies a risk for TBML/TF. This approach is similar to how an optimization works. In this respect, the less optimal a shipment is, the higher will be the complexity score. This complexity score can be used for an indication of TBML/TF before the fact as in the pre-transaction phase.

For the “through the fact” as in-progress, a shipment reasonability monitoring system could be designed based on the following information:
- Stated shipment details by the customer, including International Maritime Organization (IMO) number
- Actual shipment details provided by service providers (e.g., Llyods, International Maritime Bureau, etc.)
- Stated container details by the customer, including container number
- Actual container details provided by service providers (e.g., Global Container Shipping Platform, Searates, etc.)

Monitoring is required whether the actual shipment is consistent with the stated shipment and, if not, to what extent it is reasonable in terms of TBML/TF.

A container tracking system informs where a sea cargo is in the world and gives the port details. It is possible to track the current location of a container at any time. To track a container location, specification of the container number, bill of lading, booking number, and the shipping line are required. The International Maritime Organization (IMO) number is, however, a unique reference for ships, registered ship owners, and management companies. IMO numbers were introduced to improve maritime safety and security, and to reduce maritime fraud.

Thus, matching the container number with the IMO number is required to pair them so as to know whether a container, as stated, is being shipped with the stated ship. Through the shipment route reasonability monitoring system, any deviation from the stated route and any mismatch of a container and ship will be an indication of suspicion.

Detection of Red Flag Anomalies

As outlined in the subsection on financial crime risk management, it has been briefly mentioned what is meant by red flags, what their function are, as well as why and when red flags could be utilized. This subsection will present how red flags could be utilized with advanced analytics and artificial intelligence, as the management of these red flags in terms of, among other things,
category, number, implied risks inherent in them, sequence of control, and combination of occurrence exceed the capability of a human.

As mentioned before, in order to work on red flags, categorization, definitions, and thresholds can be selected, calculated, mixed up with each other, and calibrated in order to identify anomalies. To review, categorization of red flags can be broken down according to:

- customer (e.g., a risky small business engage in a transaction incompatible with its business size and strategy);
- transaction (e.g., transaction involving an unusual intermediary);
- structure of deal (e.g., the structure of the deal between exporter and importer appearing unnecessarily complex and designed to obscure true nature of business);
- goods (e.g., vulnerable goods traded that are not expected to be traded between countries in which trading parties are residing);
- jurisdiction (e.g., one of the trading parties is located near to the border of a risky jurisdiction);
- shipment (e.g., the shipment lacking economic sense in terms of size of goods traded and container occupied);
- document (e.g., significant discrepancies between the description of goods on the bill of lading and actual goods shipped); and
- payment (e.g., unusually favorable payment terms, such as payment substantially far above or below expected market price or lump-sum cash payment).

Because each definition of a red flag is necessarily a definition of an anomaly, the delicate issue is the determination of thresholds. For determination of thresholds, answers to the following questions should be considered:

- To what extent are the outcomes of red flags deemed to be unreasonable?
- Should the thresholds be different according to the risk of customers, and, if so, by how much?
- Does a combination of red flags imply more risk, and, if so, which combination implies more, and how much more?

- Does the risk of a red flag change if the role and position of a bank in a trade transaction change as well, and, if so, how should it be?

These and other issues about the thresholds should be decided. However, it is impossible to manage all of them manually, given the influx of data, the dynamic and complex nature of international trade, the complexity and challenges of TBML/TF, and cost and time pressure. Therefore, detection of red flag anomalies is a good use case for advanced analytics and artificial intelligence.

As indicated above, red flags can be used both through the fact as the in-progress phase, and after the fact as in the post-transaction phase. For the through the fact as in-progress phase, a red flag reasonability checking system could be designed using neural networks. As mentioned before, neural networks utilize computers to mimic how a human brain operates in learning a structure. Such a network accepts inputs, conducts an array and a sequence of operations in the data, and produces outcomes. In a set of data, in which each observation contains an input in the form of a transaction or a transfer, and a known output as suspicious or not, the network can be trained to recognize the patterns in the data. In this case, inputs are the required data defined in each red flag; the operation is the decision-making process of a human about the reasonability; and the output is the level of reasonability.

After the fact as in the post-transaction phase, by using link analysis, clustering analysis, and data visualization, a red flag reasonability monitoring system can be designed for:

- conduct of trend analysis in terms of trade transactions and trade-related transfers;
- conduct of anomaly analysis regarding the post-transaction red flags and scenarios for account activity; and
- conduct of post-event analysis for the detection of reasonability based on customer activity.
Continuous Learning and Prediction Through Analytics

The sample of opportunities for the use of advanced analytics and artificial intelligence presented above can be more detailed, extended, and enriched, which is not the aim of this work. However, to make this vision happen, live, and act effectively, the interconnectedness among these components and systems should be sustained. Because artificial intelligence learns as a human learns, interconnectedness will enable the components and systems to benefit from the experience and insight of other components and systems. If any component or system identifies any transaction or transfer as suspicious, the learning mechanism will help the others to treat the behavior of the customer or the pattern as unusual and suspicious.

As mentioned above in the subsection on approaches in advanced analytics, the sophistication level increases as it goes from descriptive analytics to cognitive analytics; and the value generated through analytics ranges from hindsight to how the human brain processes information, draws conclusions, and codifies experience into learning.

As in predictive analytics, the main goal is to find out what will happen, why it will happen, and when it will happen for a less human- and more machine-centric decision and action. The main outcome is defined as foresight and provides recommendations as an estimate of a possible future outcome. Thus, this learning experience would bring more and more value if the culmination of learning will contribute to generate hints and estimations about how the customers are more likely to behave.

If and when the sophistication and maturity of compliance technologies and analytical capabilities reach that level, the definition and management of compliance will definitely change, and the impact of compliance management on the business model of a bank will be redefined.
CONCLUSION AND FINAL THOUGHTS

TBML/TF is the largest and most pervasive methodology on the one hand, and the least understood, recognized, and enforced on the other. The complexity and challenges of TBML/TF cause FIs to be exposed to great vulnerabilities, of which they are mostly unaware. Because of the role of banks as the responsible party for combating financial crime defined in compliance programs, and the role of banks in the risk management, intermediation, and finance of trade, the effectiveness of combating TBML/TF is crucial from a regulatory perspective, but also for economic and national security purposes.

Because of its nature, traditional combating mechanisms and human-centric control structures are not effective. According to overvalued imports and undervalued exports, the estimations of the sum of money laundered are enormous, whereas, the numbers of suspicious transaction reports are still low, which imply that the compliance programs of banks are not compatible with the risks stemming from TBML/TF.

Thanks to enormous computation power, sophistication level, and availability of more data, it is no longer a dream to utilize advanced analytics and artificial intelligence, not only for TBML/TF in particular, but also for ML/TF in general. The use of advanced analytics offers new perspectives and can create value, much of which has not been tapped yet.

Recent regulatory developments encourage FIs to invest in and use advanced analytics and artificial intelligence in combating ML/TF, a domain that has not been sufficiently commercialized and widely standardized. The existing monitoring and screening systems for combating ML/TF are mainly designed with knowledge-based systems. Even a proven system, whose focus is on combating TBML/TF, does not exist in the marketplace. This implies that there is great economic potential for this domain as well. This potential can be better exploited if the existing regulatory encouragements will be continued and intensified, and if cost of compliance, both directly and indirectly, in terms of investments as well as penalties will be appropriate.

There are many use cases for advanced analytics and artificial intelligence in combating TBML/TF, which are right to the point, meaningful, and feasible. These can be implemented either before the fact as in pre-transaction phase or through the fact as in-progress phase as a preventive measure to avoid any involvement in such a crime, or after the fact as in post-transaction phase as a detective measure. Nevertheless, these use cases include detection of price anomalies, detection of weight anomalies, detection of anomalies in the profiling of traded goods for countries, detection of shipment and shipment route anomalies, and detection of red flag anomalies. There are potentially many more use cases; however, the presentation of them is beyond the scope of this work.

The vision of using advanced analytics and artificial intelligence in the compliance world, and even in combating ML/TF, is not new. However, the vision of using advanced analytics and artificial intelligence in combating TBML/TF is innovative and inspiring. I hope that the compliance community would share my vision and contribute to the realization to this vision with me.

Finally, I would like to thank Mr. Dennis M. Lormel, my mentor in this white paper, who supported, encouraged, and inspired me to work on this topic.
NOTES


4. FATF, op. cit. p. 3.


18. Ibid, pp. 24, 74-75.


28. Ibid, pp. 118-123.
33. Asia/Pacific Group on Money Laundering, op. cit., p. 44.
34. Dennis M. Lormel and Ross S. Delston, op. cit., pp. 78, 84.
38. The Wolfsberg Group, ICC, and BAFT, op. cit., p. 11.
40. The Wolfsberg Group, ICC, and BAFT, op. cit., pp. 9, 21, 69.
41. Ibid, p. 10.
42. Ibid, pp. 21, 55.
44. The Wolfsberg Group, ICC, and BAFT, op. cit., pp. 33-83.
47. The Wolfsberg Group, ICC, and BAFT, op. cit., pp. 34, 48, 61.
48. Ibid, pp. 12, 16.


50. The Wolfsberg Group, ICC, and BAFT, op. cit., p. 16.


56. Ibid, pp. 144-145.

57. Philip Russom, op. cit., pp. 6-7,18.


gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%20Cover.pdf.


WORKS CITED


Opportunities for Advanced Analytics and Artificial Intelligence in Combating the Trade-Based Money Laundering and Financing of Terrorism


