IPSA International
A root9B Technologies company

Alarming Concerns of Financial Crimes Risk in Trade Finance

New technology techniques combined with trade Red Flags needed to identify suspicious activity in trade finance conducted through Letters of Credit

February 2016 publication of IPSA's Financial Services

Table of Contents:

1. Executive Summary

The rise in trade-based money laundering (TBML), combined with the enormous regulatory fines and ongoing scrutiny from various government agencies, has created a need for enhanced financial transparency, specifically where trade finance-based money laundering (TFBML) is a subset of TBML. Financial institutions struggle to systematically create a supply chain that offers an audit trail and unhindered financial visibility to ensure the usage of an LC is not being misused or abused.

This white paper explores effective and enduring approaches to monitor and screen trade finance activities. This approach provides an all-in-one trade finance based AML monitoring, screening and reporting solution designed to address the growing complexity in trade finance monitoring so organizations can flag financial crimes activity including LC abuse, money laundering and sanctions threats.

The recommended approach recognizes the importance of key data fields in monitoring high-risk trade finance activities, understands the need to interface with current case management and screening systems, realizes the necessity of auditability, and provides reports and dashboards for investigators and officers alike.

Letters of Credit: Use and Abuse

LC history

Letters of Credit (LC) have been around for hundreds of years as it is a document from a bank guaranteeing that a seller will receive payment in full as long as certain delivery conditions have been met. An LC is normally governed by the International Chamber of Commerce Uniform Customs and Practice for Documentary Credits rules. In the event that the buyer is unable to make payment on the purchase, the bank will cover the outstanding amount. The bank representing the Buyer, or Drawee, is normally referred to as the 'Issuing Bank' and the bank that represents the Seller, or Drawer, is normally referred to as the 'Advising Bank'.

Primary use

LCs are often used in international transactions to ensure that payment will be received where the buyer and seller may or may not know each other, have not traded in the past, and are usually operating in different countries. In this case the seller is exposed to a number of risks such as credit risk and legal risk. A letter of credit provides the seller with a guarantee that they will get paid as long as certain delivery conditions have been met. For this reason the use of letters of credit has become a very important aspect of international trade.

Why use LCs rather than Open Accounts

An 'Open Account' transaction in international trade is a sale where the goods are shipped and delivered before payment is due, which is typically in 30, 60 or 90 days. Most importers prefer this option since it is advantageous to them in terms of cash flow and cost, but it is consequently a risky option for an exporter. Therefore, an LC serves the exporter's interest and guarantees payment to the supplier.

How Letters of Credit are Used and Abused to Move Illicit Funds

You will see in a recently discovered case, where established companies, owned by high level organized criminals who may have political backgrounds and connections, are utilizing LCs to move goods around the globe. This is accomplished through their own established banks or other criminal partners that share the same intention, to either hide the true and original source of funds or to maneuver around various sanctions in the world.

Regulatory bodies and BAFT

Detecting transactions that may be suspicious of LC misuse, abuse, and/or indications of money laundering, terror financing or sanctions related red flags requires a solution which must be able to effectively and primarily target red flags that are sourced from known international bodies such as FATF, FFIEC, Wolfsberg, FCA and more. Bankers Association for Finance and Trade (BAFT) recently published 16 consolidated red flags which were sourced from these international bodies. Any solution providing coverage regarding regulatory and risk in trade, minimally, must provide immediate coverage on those trade related red flags.

2. Trade Finance Challenges and Recent Cases

According to the Financial Action Task Force (FATF), an intergovernmental body with 36 member countries that sets global standards for measures to combat money laundering, terrorist financing, and other related threats to the international financial system, trade-based money laundering occurs when the proceeds of illegal activity are disguised as legitimate trade for the purposes of avoiding the original source of funds. The expansion of the global economy has led to an increase in trade-based and trade finance-based money laundering in recent years. This shift "has made international trade an increasingly attractive avenue to move illicit funds through financial transactions associated with the trade in goods[1]."

1- http://www.fatf-gafi.org/documents/documents/trade-basedmoneylaunderingtypologies.html

According to the Wolfsberg Group's Trade Finance Principles 2011 edition, "Historically, Trade Finance has not been viewed as a high risk area in relation to money laundering. This perception has changed of late and increasingly regulators and international bodies view trade finance as a 'higher risk' area of business for money laundering and terrorist financing. It should be recognized however that a majority of world trade (approximately 80%) is now carried out under 'Open Account' terms. The ability of any financial institution to understand who the ultimate buyer or seller of a product is, or the ultimate end use of that product, may be severely limited. This understanding will be even more limited where transactions are part of a complex structure[2]."

2- http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Trade_Principles_Paper_II_(2011).pdf

Furthermore, *Economist* magazine published an article from the Enforcement Directorate, an Indian agency that fights economic crime, indicating trade is "a ready-made vehicle" for dirty money. A 2012 report Enforcement Directorate helped write for the Asia/Pacific Group on Money Laundering, a regional crime-fighting body, is packed with examples of criminals combining the mispricing of goods with the misuse of trade-finance techniques. Using trade data, Global Financial Integrity, a non-governmental organization, estimates that **$950 billion** flowed illicitly out of poor countries in 2011, excluding trade in services and fraudulent transfer pricing[3]. Four-fifths was trade-based

laundering linked to arms smuggling, drug trafficking, terrorism or public corruption. This fraction equates to **$760 billion.**

3- http://www.economist.com/news/international/21601537-trade-weakest-link-fight-against-dirty-money-uncontained

Prominent Case Illustrating Letter of Credit Abuse:

Who is Babak Zanjani?

Babak Morteza Zanjani is an Iranian businessman who, according to his own statements, owns 70 companies and tens of billions of dollars inside and outside Iran[4]. He also claims he employed more than 17,000 employees worldwide and was the chairman of UAE-based holding company Sorinet Group. Zanjani's company types varied and were involved in unrelated line of businesses, such as leather and textile, jewelry, banks and financial institutions, airlines, auto parts, sporting goods, logistics, transportation, food and nutrition, tourism, building material, consulting, insurance and more. Sorinet was used by some agents of the Iranian government to finance a portion of its sales of Iranian oil and other sanctioned goods around the world. Babak Zanjani operated in Iran and Dubai and funneled hundreds of millions of dollars through his Asian banking connections, utilized lengthy tenor period LC transactions and stripped SWIFT messages to clear Iranian oil sales. A US Treasury press release dated April 11, 2013, cites the case of Babak Zanjani moving approximately $800mm of Iranian oil through LC transactions in Asia, using an intricate web of legal entities spread across multiple jurisdictions around the globe. According to the US Department of Treasury, Mr. Zanjani was designated for providing financial, material, technological or other support for National Iranian Oil Company (NIOC) and Naftiran Intertrade Company (NICO), a Swiss-based Iranian oil trading company.

4- http://en.radiozamaneh.com/articles/iranian-tycoon-babak-zanjani-arrested/
http://www.rferl.org/content/iran-zanjani-corruption-charges/25217665.html

How Zanjani utilized and abused Letters of Credit:

In a highly complex and hidden structure, International Safe Oil (ISO) was designated for providing financial, material, technological or other support for NIOC and NICO. ISO is a part of the Sorinet

Group (Zanjani's holding company), and operates in Malaysia. According to the US Department of Treasury, ISO purchased over tens of millions barrels of Iranian crude oil from NICO in 2012 in a deal that was negotiated between Zanjani and the leadership of NICO. Dubai-based Sorinet Commercial Trust Bankers (SCT Bankers), and Malaysia-based First Islamic Investment Bank (FIIB) were designated on April 11, 2013 for providing financial, material, technological or other support for NIOC and NICO.

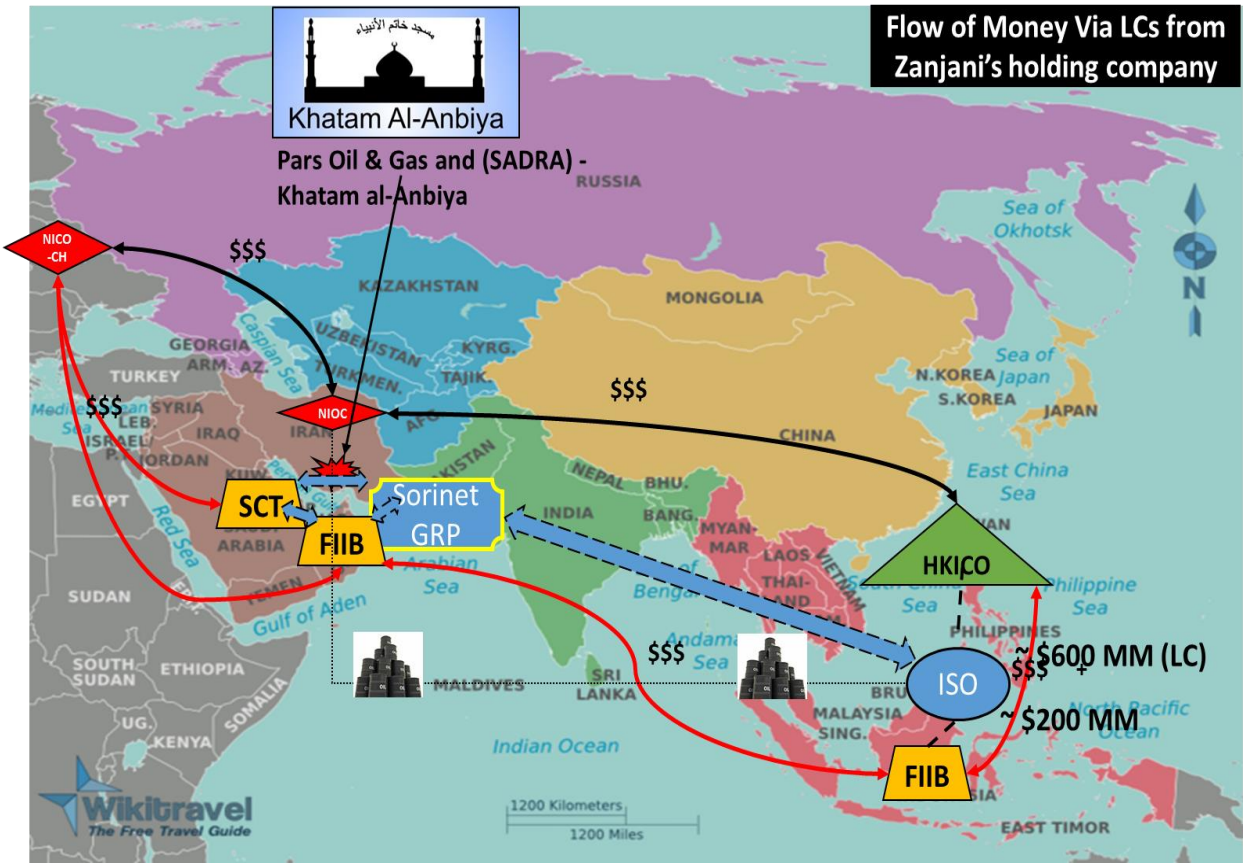

Figure 1a

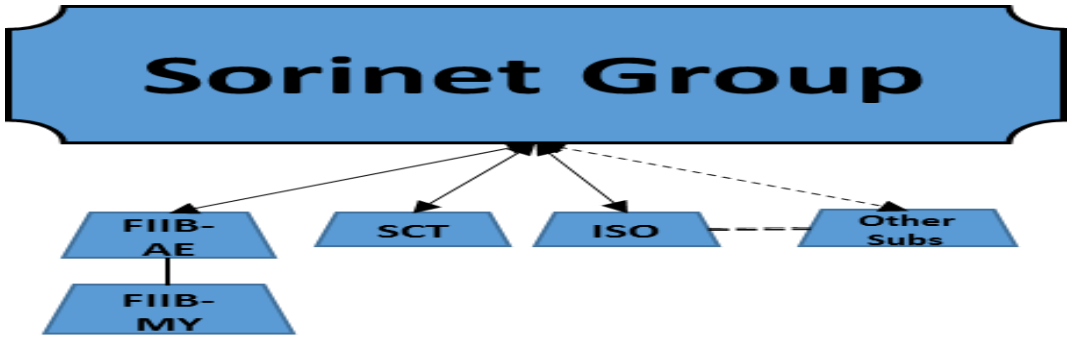

Figure 1b

August 2012, FIIB issued a lengthy tenor period Letter of Credit for Hong Kong Intertrade Company (HKICO) for almost $600 million in relation to an oil contract. HKICO was identified by Treasury as a NIOC front company in July 2012. A May 2012 oil contract negotiated by Zanjani on behalf of ISO worth over $200 million was financed by both FIIB and SCT Bankers. NICO had used FIIB and SCT Bankers to facilitate transactions worth tens of millions of dollars between Pars Oil and Gas, a South Pars Gas field development contractor in Iran, and the US-designated Iranian Marine Industrial Company, SADRA in 2012. SADRA was designated in March 2012, pursuant to U.S. state department's executive order EO-13382, for being owned or controlled by Khatam al-Anbiya, the engineering arm of Iran's Islamic Revolutionary Guards Corps (IRGC). Khatam al-Anbiya was designated in October 2007 under E.O. 13382 as an engineering arm of the IRGC that it uses to generate income and fund its operations[5]. All of these relationships are illustrated in *Figure 1a* above.

Currently, Zanjani along with a few former cabinet ministers and high level government officials are being prosecuted by the Iranian judiciary for multiple counts of financial crimes, including money laundering, bribery and fraud. Zanjani is currently being held at the notorious Iranian 'Evin' prison in Tehran, as multiple sources indicate death penalty is awaiting him.

5- http://www.todayszaman.com/anasayfa_death-sentence-sought-for-zanjani-in-irans-biggest-corruption-case_400606.html

This is illustrative of some segments of the Iranian regime's use of proxies such as Zanjani, to finance oil and other sanctioned type commodities in the international market. In some cases this was facilitated by the use of letter of credit (LC) instruments in the international financial system and companies in other parts of the world without a US nexus! Furthermore, since such oil contracts that might have been successfully settled, the illegal and sensitive commodities could then be moved through legitimate international commerce and financial systems (including the U.S.) with little or no suspicion. We should then be very concerned about the financing of the Islamic State's (ISIL and/or Daesh) oil revenues that could be occurring in a similar manner without any successful detection and trace.

6- https://www.treasury.gov/press-center/press-releases/Pages/jl1893.aspx

3. Money laundering through letters of credit?

People normally question how money can be laundered through LCs. Before we elaborate on this, it is worth mentioning how LCs are not being utilized toward its true intention and how they are being misused. It is quite a shock to learn how large corporations or holding companies, transacting in hundreds of millions of dollars annually, utilize their existing funds in banks, converting them to goods or commodities through trades to disguise the original source and its true destination. To elaborate on this, we need to understand how money laundering is structured.

There are three layers of money laundering: 1. Presentation, 2. Layering, and 3. Integration. Many technology solutions installed at institutions today are only capable of alerting red flags from the sender of funds (remitter) to the recipient of funds (receiver), pointing only to the 'payment' portion of a trade finance transaction. This, however, fails to consider there are additional parties who are realistically involved in a trade finance transaction, limiting what is captured by those systems (See *figure 2*). A more sophisticated technology approach – one that not only moves from manual

processes to an optimal, comprehensive, and fully automated digital one, that goes beyond just the sender/receiver or importer/exporter – is required. For example, a truly effective trade finance suspicious activity monitoring and screening system, focused on Export LCs, needs to integrate key trade data involved in a trade finance transaction, with related trade red flags capturing trade AML typologies to effectively address the 2nd stage of money laundering called 'layering'. It is the 'layering' stage of money laundering where existing funds in the bank will then be debited towards a letter of credit, intended to purchase certain type of goods/commodities traded that could be unaligned with the customer's profile and should be flagged for further investigation.

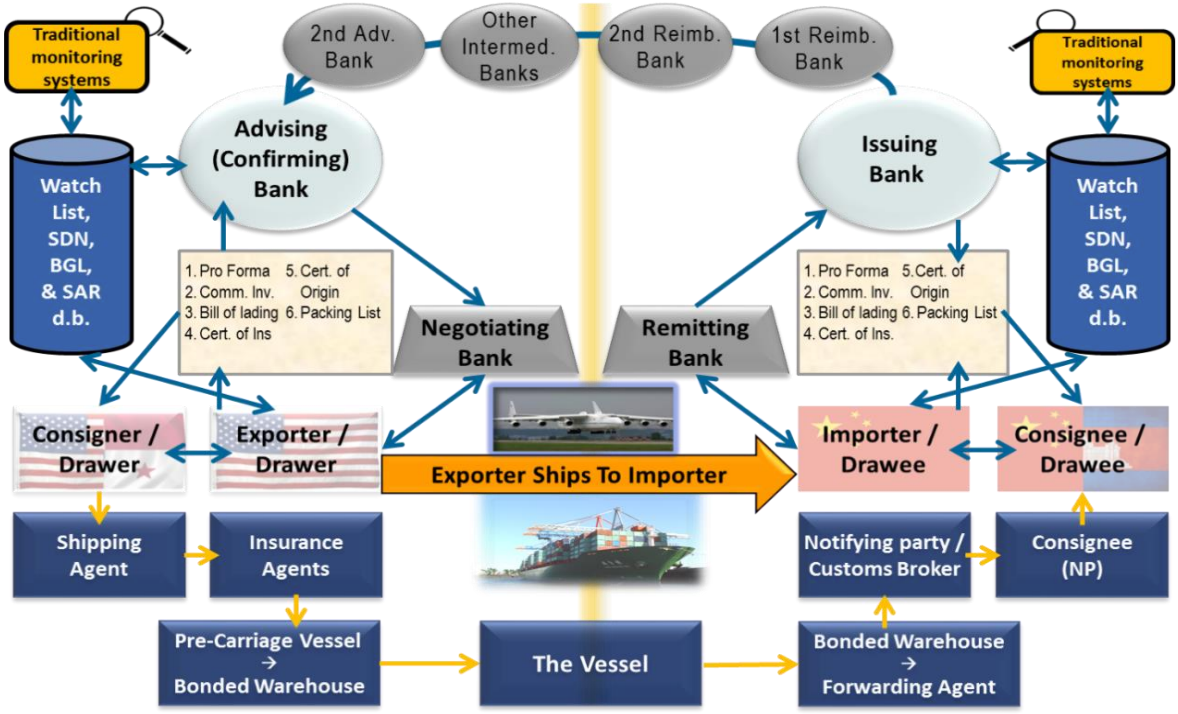

Figure 2- A complex trade finance diagram

4. Problems – How did we get here

This white paper examines the issues, challenges and risks involved in potential trade finance-based money laundering (TFBML), and why it is so crucial for financial institutions to develop and enforce appropriate policies and procedures while supporting them with the right technology. This paper also shares tips for selecting and deploying a solution to flag trade finance-based risks including money laundering, and highlights an approach that provides a robust and powerful design to help financial institutions combat this growing threat.

From a regulatory perspective, FFIEC's Trade Finance examination procedures[7] provide a guideline to an effective assessment on a financial institution's ability to manage the risks associated with trade finance activities, and management's ability to implement effective due diligence, monitoring, and reporting systems.

The assessment includes an evaluation of the adequacy of due diligence information the bank obtains, from customer account opening through current customer information updates. Examiners also review Management Information Systems and internal risk rating factors, and make determinations on whether the bank effectively identifies and monitors trade portfolios for suspicious or unusual activities, particularly those that pose a higher risk for money laundering. Additionally, the procedures help determine whether the financial institution's systems for monitoring trade finance activities for suspicious activities, and for reporting of suspicious activities, are adequate, given the bank's size, complexity, location, and types of customer relationships.[8]

7- https://www.ffiec.gov/about.htm
8- https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_080.htm

5. Challenges of Trade Finance Monitoring

In order to identify unusual and suspicious activities in trade, financial institutions must rely on a number of different data sources. For example, the LC records themselves must be related and linked to the presentation records (i.e. Bill records) from various sources associated with that particular LC. The trade data related to a particular transaction must include: a 'unique identifier' such as an LC number. Consider this 'unique identifier' to be a red nail, in a sort of -- needle in a haystack -- which represents the ground zero of all trade's 'dirty data' of your trade database and trade booking systems *(See figure 3)*. This red nail will be the pivoting factor around retrieving all related data to a trade deal.

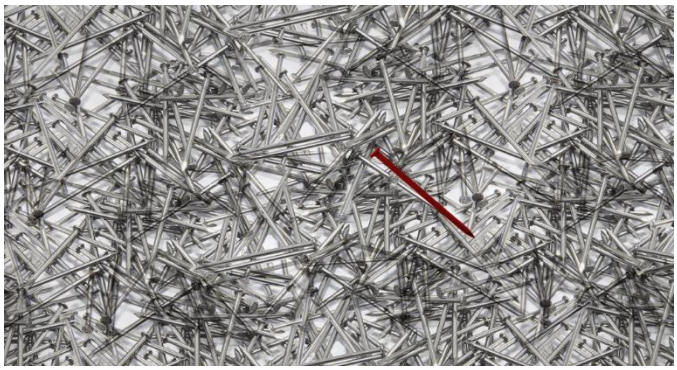

figure 3

Additionally, key trade fields such as the Exporter/Drawer Name and Address, Importer/Drawee Name and Address, Ship To, Ship From, relevant Ports involved, LC amount, Currency, Tenor period, Goods being shipped and more, along with relevant risk rating tables such as country ISO codes, OFAC sanctioned seaports, Internal watch-lists, SDN lists, Goods codes and their risk rates, Subsidiary names and their percentage of ownership from bank's KYC database, and more, are data that should be captured to accurately monitor and process each trade transaction.

6. Trade Finance-Based Money Laundering (TFBML): The Issues and Challenges

Suspicious activities could occur in various ways during the LC process. A few examples are provided below to better understand how this is accomplished:

1) ***Deviation From Profile*** **-** This is where there is a violation against a customer's "expected activity". In this scenario a trader/customer has a registered and certified Know Your Customer (KYC) profile with their financial institution, indicating that trading certain goods and within certain jurisdictions in the world are under a certain monthly dollar amount with quantity volumes. Expected activity is the norm. When a trader steps outside that norm, it is considered unusual and suspicious. For example, imagine a trader normally trades in canned food with a volume of approximately $10,000 a month and consistently ships these goods to East Asia. This is considered their expected activity. Now, imagine if that the same trader suddenly begins trading exotic cars with a volume of approximately $500,000 a month to high-risk countries in the Middle East. This would be considered suspicious and an investigation should take place. Current manual coverage is challenged when the volume of these transactions are high, and makes it even more difficult when you constantly need access to many customer profiles. It is now worth referring to the case of Babak Zanjani's company 'ISO' and its past history and profile, where an alert can display the high volume, and the high risk commodity of Oil trade deal in relation to its past history.

2) ***High Risk Patterns*** **-** The ability to immediately flag transactions that contain 'patterns' of multiple high risk indicators in a trade deal. For example when a trade LC contains a high risk country of 'Ship To', such as Libya involving goods that are considered high risk, such as precious metals with a round and very high LC amount, the transaction needs to be reviewed more closely.

3) ***Standby LC Payment Recurring*** **-** A beneficiary of a Standby LC (SBLC) keeps receiving funds in various regions within your institution's global banking system in short time frames. Hence the financial institution needs to investigate this beneficiary which may impact the relationship. Institutions needsa robust system to ensure defaulted beneficiaries on SBLCs are captured in their global banking system.

4) ***Exclusive Relationship*** **-** An exclusive relationship exists when an exporter has a history of high-volume dealing and trading with only one importer and/or is dealing with that singular importer by trading goods in different categories and, usually, with high-dollar volumes. Under AML guidelines, and with the exception of certain exclusions, both entities are considered suspicious and should be subject to an investigation. Enhanced due diligence with respect to these transactions may result in escalation and the generation of a Trade Suspicious Activity Report (SAR). Again it is worth referring to Zanjani's Sorinet Group's transactions with its subsidiaries and National Iranian Oil Company-NIOC.

There are many additional trade red flags that currently are being monitored manually, and due to large transaction volumes there are gaps in control and potential for errors. Those examples include:

Match / Mismatch Red Flags	Unusual and Suspicious Events
Business Address Mismatching Ship To/From	Deviation On Goods In Trade
Ports Mismatching With Ship To/From	Deviation On Countries In Trade
Matching Names and Addresses	Deviation On Countries In Trade
Non-Business Account Deposits	Deviation From Currency and Transaction Range

LC-Bills Mismatch	Double-Invoiced Transactions
	Obvious 'Over and Under' Invoiced Transactions
Screening and Monitoring	One-Off Trades
Full Sanctioned Seaports and Free Zones	Unusual Amendments
Non Standard Trade Clauses	Exclusivity
SWIFT Monitoring	Same Country LC
Vessels and Dual Use Goods Searching	
Percentage of Ownership Awareness/Flagging	

7. Compliance Issues and the Costs of Non-Compliance

The Financial Crimes Enforcement Network (FinCEN) and The Office of Foreign Assets Control (OFAC), a part of the U.S. Department of the Treasury, are responsible for ensuring financial institutions remain in compliance with trade regulations with respect to money laundering and sanctioned entities. When regulators have found that a financial institution or other institution responsible for trading with sanctioned persons or countries has committed a violation, they either reach a settlement with the institution or, if a settlement cannot be reached, fine that institution. Recently, numerous domestic and foreign banks have been subject to heavy fines in the millions and billions of dollars. These are the types of penalties institutions are subjected to when they fail to properly monitor and control potentially illegal activities in their trade transactions.

Recently, New York Governor Andrew Cuomo announced anti-terrorism regulation requiring senior financial executives to certify effectiveness of anti-money laundering systems. The new rules, among the nation's strictest, would require senior financial executives to certify *personally* that their institutions have strong safeguards to identify, weed out and prevent illicit transactions. Violations potentially could subject the officials to legal penalties[9].

[9] *http://www.dfs.ny.gov/about/press/pr1512011.htm*
http://www.usatoday.com/story/money/2015/12/01/ny-proposes-tougher-anti-money-laundering-regulations/76609730/

8. Technology -- compliance challenges and how do we fix them

The solution provided introduces the ability to associate disparate data into comprehensive transaction/client relationships; standardize the investigative process and create a baseline for consistency; identify current customer activity against their historical profiles, including their trading patterns; and enhance trade monitoring that can utilize an entity's risk profile and apply greater scrutiny to mitigate risk in an institution.

Addressing Technology Challenges

Linking multiple systems to retrieve key and relevant trade data that are not linked to each other. Those include:

- Letter of Credit records
- Presentation records
- SWIFT Messages

- ISO Country Codes
- Goods Risk Rating tables including Dual Use Goods
- Customer Risk Rates
- Trade Finance Product Risk Rates
- HIDFA and HIFCA - High risk U.S. states lists
- SDN lists
- Full Sanctioned Seaports
- Internal Watchlist
- Captured values from OCR forms scanned
- Etcetera

Trade Finance Data Mastering

Automate access, retrieval and parsing of data from all associated trade tables, databases, records, and all associated risk-rating tables to understand and manage trade data more effectively via:

- **Enhanced data quality** – To develop rules that identify errors and even "correct" trade data errors in fields such as addresses, countries, misspellings, character substitutions, etc. (e.g *Chino* to *China*).
- **Matching rules** – To utilize automated logic to match different trade transactions together based on a common set of fields and attributes.
- **Merging** – To combine information from multiple internal systems such as customer KYC and transactions booking systems to create an "enriched" transaction record.
- **Transformation** – To analyze Trade transaction data to convert, aggregate or enhance data for use in monitoring.

  Example: "Transform" or roll up Port of Arzew, Cherchell and Skikda to the high risk jurisdiction of Algeria.
- **Validation** – To utilize technology programs to confirm all data quality enhancements, record matching and merging rules detailed above are appropriate and implemented accurately.

Due to the capabilities mentioned above, false positives should drastically be reduced.

Compliance Challenges

- Augmenting Know Your Customer information and strategy
- Enhancing customer due diligence capabilities
- Struggling to improve the financial transparency of the trade program
- Ensuring that monitoring software supports the new standards and practices mandated by regulators
- Having a robust set of risk rating tables relevant to trade monitoring
- Screen ALL relevant trade data in a trade finance transaction.

9. Recommended Approach

A solution is required to be technology based and driven on a framework that introduces four pillars to this challenge:

- **Alerts-** The first pillar of the methodology provides for an alert-based mechanism to give investigators a rapid view of flagged suspicious activity.
- **Reports-** The second pillar of the methodology includes reports and dashboards for trade compliance and business executives.
- **Random Sampling-** The third pillar of the solution provides the ability to dynamically select random transactions to examine or investigate.
- **Case Management Tool (CMT) -** The final pillar of the solution is an interface to the institution's existing case management facility (CMT).

10. Conclusion

Today, most financial institutions use traditional surveillance analysis software programs to monitor and screen transactions. These programs, however, lack the features and functionality needed to effectively flag suspicious activities in each and every party involved in a trade finance transaction particularly letters of credit.

A successful solution needs to minimally execute majority of trade red flags published in known international bodies such FATF, FFIEC, Wolfsberg, FCA and more, where BAFT (Bankers Association for Finance and Trade) recently sourced and published 16 trade red flags as a consolidated list pertaining to the most important red flags. A confident and robust solution needs to provide immediate and minimum coverage on those red flags.

Moreover, a chosen solution must be a comprehensive analytics and reporting solution that enables views of concentrated risk across entire, or components of, trade portfolios. It should be a monitoring solution that highlights potentially suspicious activity at the individual deal or transaction level.

Analytics can be utilized to spot trends at customer profile, trading partner, trade route and commodity levels. When considering geo-political occurrences in the world, analytics will provide a useful risk based approach by displaying the needed information. Financial institutions may need to apply a risk-based approach that seamlessly connects Letter of Credit (LC) and Bill/Presentation record data with relevant risk rating tables to mitigate risk across the program. A platform is required to monitor, screen and provide analytics which enable financial institutions to:

- Alert stakeholders when problems arise
- Improve financial crimes risk management across the trade finance program
- Automate flagging of unusual activity against Trade AML typologies
- Standardize trade programs with affiliates and correspondents
- Identify sanctions risks (including seaports) beyond customary screening systems
- Establish a global bank-wide repository of all critical issues to both improve your business and compliance
- Provide the ability to screen SWIFT messages from four different perspectives: a) Sanctions Screening, b) Non-standard clauses, c) Mismatching with key Trade Parties and d) Non-Trade related SWIFT messages
- Interface with the institution's existing Case Management Tool

- Integrate related sources such as Automatic Identification System (AIS) and The Journal of Commerce (JoC) to track Vessels worldwide
- Extensive, inherent user and data security capabilities to safeguard sensitive customer and transaction information
- Avoid human errors and omissions in identifying trade red flags
- Improve customer due diligence and Identifies trade activity out of pattern with existing KYC customer profiles
- Make aware and trains trade personnel

Whatever the approach chosen, it needs to be an all-in-one, comprehensive trade finance-based monitoring, screening and reporting solution designed to address the growing complexity in trade finance monitoring. Organizations should be able to flag trade related suspicious activities. A robust solution is needed to recognize the importance of key fields in monitoring and screening high-risk trade activities, and to understand the need to interface with the institution's case management system. An approach must realize the necessity of random sampling, and to provide reports and dashboards for investigators and officers alike.

For more information contact:
Ehsan Valipay, CAMS, Senior Consultant,
IPSA International
A root9B Technologies, Inc company
Cybersecurity and Regulatory Risk Mitigation
Email: evalipay@ipsaintl.com
Mobile: 917-977-1253