ACAMS White Paper

How to Effectively Audit Financial Crime Risks in Trade Finance in a Complex Regulatory Environment

1. Introduction

Trade finance is considered a high-risk product often used by bad actors and criminal organizations to launder funds, conduct terrorist financing and evade Office of Foreign Assets Control (OFAC) sanctions regulations or other restrictions. Banks that provide trade finance services are under significant regulatory pressure to develop consistent standards across the complete suite of trade finance products to mitigate financial crime risks.

The Financial Action Task Force (FATF), the Wolfsberg Group and the Joint Money Laundering Steering Group (JMLSG) have all drawn attention to the misuse of international trade finance as one of the ways criminal organizations and terrorist financiers move money to disguise its origins and integrate it into the legitimate economy.

This white paper will address financial crime compliance (FCC) risks, red flags and best audit practices for identifying control deficiencies and risk mitigation in the trade finance business.

2. Regulatory Environment

Many customs agencies, law enforcement agencies, financial intelligence units (FIUs), tax authorities and banking supervisors (i.e., competent authorities) appear less capable of identifying and combating trade-based money laundering (TBML) than they are in dealing with other forms of money laundering and terrorist financing.

Furthermore, the complexity of transactions and the huge volume[1] of trade flows have placed increasing pressure on the limited resources that most countries, especially developing countries, have available to scrutinize these activities.

As the standards applied to other money laundering techniques become increasingly effective, the use of TBML can be expected to become increasingly attractive.

The recent report by the Financial Conduct Authority (FCA), highlighted a number of common weaknesses in their review of 17 banks in the U.K. involved in trade finance activities, illustrating how increasingly vulnerable financial institutions are to financial crime risks (Refer to Appendix 1 for more details of the FCA findings).

3. Definition of Trade Finance Products FCC Risk Ranking

---

[1] *Global trade merchandise now exceeds USD9 trillion a year (Source: Financial Conduct Authority - Banks' Control of Financial Crime Risks in Trade Finance - July 2013)*

Trade finance refers to the use of short-term financing to facilitate the import and export of goods. Such arrangement can involve payment if documentary requirements are met, such as through the use of letter of credit, or through a commitment to make payment in the event the original party with the obligations defaults on the terms of the transactions (through the use of guarantee or a standby letter of credit). Most trade financing is short-term and self-liquidating

A brief description of common types of trade finance products is provided below.

3.1 *Common Trade Finance Products* [2]

Letter of Credit (LC): The most widely used trade finance instrument, is a formal commitment issued by a bank on behalf of and at the request of a customer, to pay a named beneficiary a stipulated amount of money upon presentation of specified documents set out in terms and conditions detailed in the letter within a specified time frame. There are two types of LC:

- **Documentary or commercial LC:** Mostly used to finance a commercial contract for the shipment of goods from seller to buyer by providing for the prompt payment of money to the seller when shipment is made as specified under its terms.

- **Standby Letter of Credit (SLOC):** Guarantees payment to the beneficiary by the issuing bank in the event of default or nonperformance by the account party the bank's customers. Although an SLOC may arise from a commercial transaction, it is linked to the shipment of goods from seller to buyer.

Irrevocable LC: Commitment by the issuing bank to pay, provided that the beneficiary complies with the terms and conditions of the LC that cannot be changed unless all parties agree. Conversely, revocable LCs can be cancelled or amended without notice to the beneficiary.

Confirmed LC: An LC guaranteed by a second bank, in addition to the bank originally issuing the credit. The confirming bank agrees to pay or accept drafts against the credit even if the issuer refuses.

[2] *Source: Protivity - Guide to US Anti- Money Laundering Requirements – Frequently asked questions- November 2012*

Back-to-Back LC: An LC on the strength of another LC of credit involving a related transaction and nearly identical terms.

Banker's Acceptance (BA): LCs may require payment at sight (at the time the documents are determined to be in order) or alternatively allow a deferred payment at a specified future date (upon expiration of a stated issuance period such as 30, 60, 90 days, etc.). Once documents presented under a deferred payment LC are determined to be in order, or the importer has waived any discrepancies, the LC is reversed and a BA is created with the appropriate due date. This BA is recorded as both an asset to record the receivable from the importer and a corresponding payable to record the bank's obligation to the exporter. As with LCs, banks are obligated to pay the exporter at maturity irrespective of whether reimbursement is received from the importer

Shipping Guarantee: In most instances, especially with ocean shipments, shipping documents are received by the issuing bank at or prior to the arrival of the vessels carrying the goods. This allows the issuing bank to properly process the documents and remit them to the importers in sufficient time for them to secure the goods. However, in some instances, primarily with air shipments, the goods arrive first. In these cases, importers may be anxious to secure release of the goods to avoid storage/demurrage costs or satisfy the demands of their buyers. To induce steamship companies or airlines to release goods in the absence of the actual shipping documents, the issuing bank will issue either a shipping guarantee or air waybill release; the liability is marked against the importers line of credit.

Documentary Collection: Banks facilitate the exchange of goods for payment without any financial obligation or engagement on their part.

Open Account Trading: Unsecured trade transactions in which the buyer and seller agree on the terms of the contract. Goods are delivered to the buyer, who then arranges payment through the financial system. Goods are shipped before payment is due (typically within 30 to 90 days). The majority of trade transactions are executed in this fashion as opposed to financing involving prepayments, collections, LC, etc.

Refer to Appendix 2 for a description of the various roles banks can take in trade finance transactions.

3.2 *Product Risk Ranking and Justification*

The table below defines the FCC risk ratings (High, Medium) and justification for trade finance products:

Product	FCC Risk	Risk Justification
Documentary Credits (Advised/Confirmed/Transferable/ Irrevocable/Back to Back)	High	Products that support the movement of goods services and funds across borders
Documentary Collection	High	Products that support the movement of goods services and funds across borders
Open Account Trading	High	Products that support the movement of goods services and funds across borders
Bankers Acceptance	High	Products that support the movement of goods services and funds across borders
Shipping Guarantees	Medium	An ancillary product emanating from a DC or a collection
Standby Letters of Credit (LOC)	Medium	SLOCs do not always cover the movement of goods internationally, they frequently support financial arrangements.

4. Red Flags in Trade Finance

Red flags are a key component to be used as a starting point for detecting potential suspicious activity in trade finance transactions. This section describes common trade finance FCC red flags, as well as the overall audit approach to assess their effectiveness in monitoring trade transactions "in flight."

4.1 *Trade Finance Red Flags*

The following table provides a list of FCC red flags that should be considered by trade finance processing staff when monitoring transactions "in flight:"

Red Flags	
1.	Items shipped that are inconsistent with the nature of the customer's stated line of business
2.	Shipment locations of the goods or shipping terms on the transport document if available, are inconsistent with the LC
3.	Request for proceeds of the transaction to be paid to an unrelated or unexplained third party
4.	Re-submission of any document by a customer rejected due to financial crime risk
5.	Applicant is overly keen to waive discrepancies
6.	Beneficiary name indicates potential military involvement
7.	Suspicious client contact, for example: - The client requests an unusual degree of confidentially - The client is reluctant to provide clear answers to routine questions - Inconsistent, false or potentially suspicious information provided - Excessive, aggressive or pressured contact by the client
8.	Obvious over-or underpricing of goods and services
9.	Transactions involving high-risk goods (e.g., weapons, ammunition, chemicals, sensitive data, nuclear materials, precious gems, crude oil)
10.	Goods are transshipped through one or more jurisdictions for no apparent economic reason
11.	Missing trade documentation information, such as: - Names and address of applicant/beneficiary - Name and address of issuing bank/advising bank, - Specified or determinable amount and type of currency - Sight or time draft to be drawn, expiry date, general description of merchandise - Types and numbers of documents that must accompany the credit
12.	Unwillingness to provide documents to prove the shipment of goods
13.	Transactions structure appears unnecessarily complex and designed to obscure the true nature of the transaction
14.	Documentation showing a higher or lower value or cost of merchandise that was declared to customs or paid by the importer
15.	Documentary fraud
16.	Changes in payment instructions
17.	Excessively amended LCs
18.	Presentations of letters or documents where the financial institution has no record of the credit's existence
19.	LC that includes a condition for a "switch bill of lading"
20.	Bill of lading describing containerized cargo, but without a container numbers or with sequential numbers
21.	Invoice showing miscellaneous charges, (e.g., handling charges greater than 40 percent of total invoice)
22.	Transaction involving front/shell companies

Source: Protivity - Guide to US Anti- Money Laundering Requirements – Frequently asked questions- November 2012

4.2 *Auditing Trade Finance Red Flags*

In order to assess the adequacy, application and effectiveness of the FCC red flags listed in section 4.1, the auditor should perform the following:

1- Verify that the business has identified the appropriate red flags in their portfolio for all products offered. Refer to section 3.1 for a sample of trade finance products.

2- Verify the red flags have been reviewed and approved by an AML governance committee and senior compliance management.

3- Ensure the red flags are validated at least annually or more frequently if there has been a breach of control. Changes to red flags must be approved by senior compliance management.

4- Through inquiry and observations, verify the red flags are being used as intended by trade processing staff responsible for reviewing/approving transactions. Ensure the red flag reviews are documented by processing staff and evidenced (i.e., sign off).

5- Ensure that once red flags have been identified in a trade finance transaction, they are being escalated by trade processing staff. Escalations should be documented, indicating when and to whom, and the final results of the escalation. All these dates should be formally documented in a log available for review.

6- Select a risk-based sample of transactions, looking at logs, to ensure we agree with final decisions that items did (or did not) meet the requirements of a red flag, and whether it should have been escalated or not.

7- Ensure that appropriate timely risk remediating actions have been taken on escalated transactions.

8- Ensure there is quality assurance (QA) process by management or compliance to make sure that trade processing staff are using these red flags.

5. Operational Considerations, Controls and Risks

The need for strong internal controls is fundamental to managing financial crime risks related to trade finance. However, the involvement of multiple parties on both sides of any international trade transaction exacerbates the challenges in establishing robust controls. This section describes some of the key controls, risks and examples of simple and complex TBML techniques.

5.1 *Key Controls*

- The establishment of clear policy or procedure documents for dealing withTBML risks to identify potentially suspicious transactions.
- Comprehensive policies and procedures that are inclusive of defense trade laws and regulations and outline the procedures for dealing with licensing and compliance matters such as:
  - Procedures for screening customer, carriers and countries
  - Screening procedures for high-risk transactions to combat illegal exports/retransfers
- The production of management information on financial crime risks in the trade finance business.
- Sufficient time must be provided to sanction alert teams to fully investigate potentially suspicious activity, particularly when there are commercial time pressures.
- The existence of clear escalation procedures when potential hits are identified.

5.2 *Key Risks*

TBML is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Below are examples of basic and complex TBML techniques:

5.2.1 Basic TBML Techniques

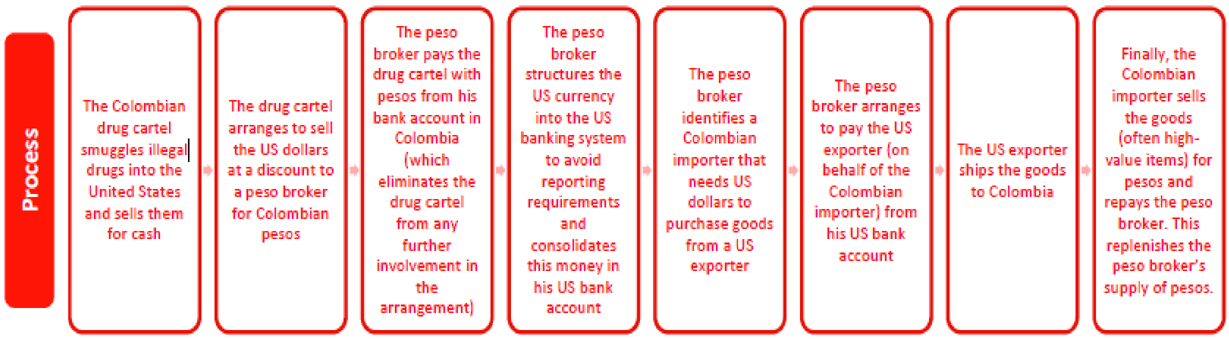
- Dual use goods
- Over / Underinvoicing of Goods and Services
- Multiple Invoicing of Goods and Services
- Over / Under Shipments of Goods and Services
- Falsely Described Goods and Services

5.2.2 Complex Money laundering Techniques

Criminal organizations continue to develop new and complex methods to abuse the financial systems to launder their illicit funds and evade detection from competent authorities. One such method is through the use of Black Market Peso Exchange (BMPE) arrangements described below.

Black Market Peso Exchange Arrangements (BMPE)

The mechanics of BMPE arrangements became the subject of considerable study in the 1980s when Colombia became the dominant exporter of cocaine into the U.S. These illegal drug sales generated about $10 billion a year for the Colombian drug cartels, of which as much as $4 billion[3] a year was laundered through black market peso arrangements. The mechanics of a simple BMPE are as described below:



Source: From FATH GAFI – TRADE BASED Money Laundering – 2006

6. Sanction Screening and Investigations

An effective sanctions screening program is essential to manage sanctions risk in trade finance. Automated screening should be used in conjunction with manual screening, given the challenges associated with automated screening. Refer to 6.2 for more details of challenges posed by automated screening solutions.

6.1 OFAC Risk for Trade Services

The greatest risks for trade finance from an OFAC perspective are:

- Transnational Criminal Organizations
- Non-proliferation (NPWMD)
- Conflict diamonds
- Burma (Myanmar)
- North Korea
- Sudan
- Syria
- Cuba

[3] *Source: FATH GAFI – TRADE BASED Money Laundering – 2006*

- Iran

6.2 *Challenges*[4]

Trade finance transactions present some challenges for banks when carrying out sanction screening that could hinder full compliance with OFAC regulations, including the following:

- Trade files are paper based and require manual input to screening systems
- Numerous parties located in foreign jurisdictions
- Frequent amendments during the life of the deal (e.g., changes to involved parties)

6.3 *Automated Screening*

- Automated screening consist of screening against a blacklist database comprising organizations, individuals, goods, vessels and countries compiled by regulatory-competent authorities.
- The system works by measuring the resemblance between blacklisted entries and applicable fields on the trade transaction, matching within a similarity threshold flagged as a possible "hit."
- Screening is directly dependent on the quality of data input.
- Given the large section of text that can be found on trade documents, it is essential that no critical information fields are omitted when inputting trade transactions. In some cases manual screening may be necessary due to field size limitations. Refer to section 6.4 for cases where manual screening is necessary.

6.4 *Manual Screening*

Should be used in conjunction with automated screening:

- If field size limitation does not allow to fully input the information, the data must undergo manual screening
- Where trade documents are submitted in foreign languages
- Automated screening utility is not available or the system is down

6.5 *Sensitive Words Screening*

Screening should also be done against sensitive words, including the following terms:

- Armored Combat Vehicle Artillery Attack Helicopter
- Ballistic Battle Tank Bomb

[4] *Source: Protivity - Guide to US Anti- Money Laundering Requirements – Frequently Asked Questions- November 2012*

- Bullet Care Sanctioned Country Centrifuge
- Combat Aircraft Diamonds Do Not Mention
- Dynamite Explosive, Grenade
- Steel Military Missile
- Munitions Nuclear One of Our Customers
- Terrorism Uranium Warship
- Weapon, Zirconium

6.6 *Investigations*

Investigation is required in the event of a potential hit with the aim being to conclude whether a real or false hit has been identified, and whether formal reporting to the U.S. Department of the Treasury (OFAC) is necessary. If reporting is required, banks must submit the report to OFAC within the applicable timescales set by OFAC.

7. Audit Approach—Trade Finance FCC Risks

Key audit points to consider when conducting reviews of FCC risks within Trade Finance activity:

7.1 *Control Description*

Ensure the customer is in good standing and a complete customer KYC (including the performance of a recent site visit) is recorded prior to onboarding customer.

Audit Approach

- Select a risk-based sample of new trade customers to ensure that a properly completed KYC is on file, along with the KYC certification.
- Ensure that appropriate documentation exists to support customer names, addresses, site visits, the tenor company has been in business, produce and services offered, etc.
- Ensure that discrepancies and omissions with respect to CIP/KYC are properly resolved.
- Ensure that no trade activity is conducted until KYC discrepancies are resolved.

7.2 *Control Description*

Ensure clear trade finance policy and procedures are maintained. These procedures should be revised at least annually (or more frequently as needed) with revisions approved by the head of the business and senior compliance management. Staff should certify in writing that they have read and understand these procedures.

Audit Approach

- Verify trade finance AML procedures were updated and approved.
- Select a sample of employees and ensure that their certifications are on file.

7.3 *Control Description*

Ensure that transactions have been reviewed against specific red flags, and where necessary escalated to supervisors for further analysis, followed by further referral to compliance where necessary.

Audit Approach

- Interview a sample of staff to ensure they are familiar with the procedures and red flags.
- Review a risk-based sample of trade finance transactions and ensure FCC red flag warning lists are attached to the copy documents and completed in accordance with procedures.
- Review a sample of items that have been escalated to compliance due to FCC red flags for proper disposition. Confirm a timely response is received from compliance and appropriate action has been taken in accordance with their guidance.
- Sample a random selection of transactions across all products. Check copy documents and transaction record for red flags (where referral has not occurred) to ensure that referral is happening where appropriate.
- Determine whether a suspicious activity report (SAR) is filed in a timely manner with the Financial Crimes Enforcement Network (FinCEN) as appropriate.
- Ensure that where required by local regulation the customer's account/assets are blocked and reported to OFAC.

7.4 Control Description

Ensure that discreet due diligence is undertaken on relevant counterparties, with whom trade finance transactions may be conducted.

Audit Approach

- Review the database of customers where the business has completed due diligence and ensure that the due diligence has been refreshed within the last 12 months.
- Sample a number of counterparties to ensure that the due diligence has been undertaken with appropriate escalation as necessary.
- Determine whether counterparties are placed on appropriate "watch list" as deemed necessary to monitor future activity.

7.5 Control Description

Verify that automated sanctions screening is performed on trade transactions during the life of the deal. Where genuine hits are identified, ensure they are escalated for further investigation and reporting, and where obvious false hits are identified, determine whether these can be overridden by the approver.

Audit Approach

- Review a sample of transactions to ensure that screening procedures are being followed and evidenced of the checks maintained.
- Review the screening systems[5] used by banks to ensure that the system parameters are set correctly and exact match is turned off (partial match is preferred though it will result in greater false positive volume).
- Test system functionality by undertaking a sample of dummy transactions, across all products, using actual sanctioned names, obtained from U.S. Department of the Treasury (OFAC) sanctioned list, to ensure that hits are flagged, providing assurance that these sanctioned names would trigger a hit. Caution should be exercised when conducting this test to avoid corrupting production environment. This a routine Computer Assisted Audit Technique (CAATS) best performed in collaboration with the CAATS team.
- Review system input, and observe the inputters and approvers to ensure that the mandatory fields are being completed and the process for overriding false positives is being followed.

7.6 *Control Description*

Ensure manual sanctions screening is utilized to supplement automated screening. In the absence of automated screening, manual sanctions screening must be undertaken by screening names against blacklist databases and maintaining paper records of screening results as evidence.

Audit Approach

- Review a risk-based sample of trade finance transactions to ensure that the manual screening procedures are being followed and evidence of the checks is maintained.
- Review the use of screening systems or databases to ensure that the system parameters are set correctly and exact match is off.

7.7 Control Description

5 Banks commonly use a vendor based screening system or database to efficiently conduct background checks on their clients to ensure they have never been involved in any form of money laundering or other illicit activity that would prohibit them from becoming a customer.

Determine whether a “good guy” list is maintained, and evaluate change management process surrounding this list. The screening solution will allow for names to be loaded as "Good Guys," to ensure these names do not unnecessarily flag as a possible hit, thus reducing the number of false positives.

Audit Approach

- Obtain a list of good guys loaded into the automated screening system; select a sample of names, to confirm that these have all been approved by senior compliance management.
- Interview management to understand their process for good guy management ensuring that it is being completed on a regular and timely basis.

7.8 ***Control Description***

Ensure staff complies with U.S. Anti-Boycott laws[6] and non-proliferation export requirements. DCs containing wording that supports illegal embargos and/or goods that can be used to produce weapons of mass destruction (WMDs) are referred to legal and compliance for resolution.

Audit Approach

- Test a risk-based sample of trade transactions (covering all products) to ensure that associated documentation contains evidence (compliance stamp) that Anti-Boycott and non-proliferation compliance steps were performed by the processors.
- Review of the underlying transaction to ensure that wording and goods do not present compliance exposures that were missed.

7.9 ***Control Description***

Ensure adequate metrics are maintained on sanctions hit ratio, including total alert volume, escalated items, true hits, etc. Obtain monthly reports showing the number of hits identified to ensure there has been no significant deviation in hit rates, month on month (e.g, > 10 percent).

Audit Approach

- Review reports to ensure that hit ratios are within acceptable parameters.

[6] *Source: US Department of Commerce: During the mid-1970's the United States adopted two laws that seek to counteract the participation of U.S. citizens in other nation's economic boycotts or embargoes. These "Anti-Boycott" laws are the 1977 amendments to the Export Administration Act (EAA) and the Ribicoff Amendment to the 1976 Tax Reform Act (TRA).*

- Investigate significant deviation and obtain satisfactory explanation from management.

7.10 ***Control Description***

Confirm that trade finance staff have taken appropriate OFAC training at least on an annual basis.

Audit Approach

- Verify that instructor lead OFAC training was provided to operations and all key staff were in attendance.
- Examine attendance records for a sample of employees.

APPENDIX 1—Common Weaknesses Identified by the FCA[7]

Common weaknesses identified by the FCA arising from their review of 17 banks in the U.K. involved in trade finance activities, conducted during September 2012 and July 2013, included the following:

- Inconsistent approach to risk assessment and only a few banks had conducted specific trade finance money laundering risk assessment. With the exception of dual-use goods, banks generally had a more sophisticated, mature and better defined approach to managing the risk of sanctions breaches than to managing money laundering risk.

- About half of the banks had no clear policy or procedures document for dealing with TBML risks. As a result, some banks failed to implement adequate controls to identify potentially suspicious transactions.

- Many banks were unable to demonstrate that money laundering risk had been taken into account when processing particular transactions. In particular, trade processing staff in most banks made inadequate use of customer due diligence (CDD) information gathered by relationship managers or trade sales teams. However, a minority of banks used some innovative and effective techniques to assess money laundering risk in trade finance transactions, which other banks could usefully follow.

- Most banks produced little or no management information on financial crime risks in the trade finance business.

- Many banks, particularly smaller banks, had not developed specific trade finance financial crime training for relevant staff. As a result, we found evidence of staff failing either to make appropriate enquiries about financial crime risks or to escalate potentially suspicious transactions. Many banks relied heavily on the fact that trade processing staff were generally very experienced, but we often found they were not considering money laundering risk in practice.

- Limited evidence that banks were escalating potentially suspicious transactions for further review and more senior level sign-off on the basis of money laundering concerns. Transactions were usually escalated for sanctions reasons or because the value of the transaction had exceeded a pre-determined threshold.

- Systems and controls over dual-use goods were inadequate at most banks.

- Some banks need to do more work to assess whether staff are exercising the right judgments when closing down sanctions alerts, and others need to ensure that all entities involved in a transaction are appropriately screened.

---

[7] *Source: Financial Conduct Authority - Banks' Control of Financial Crime Risks in Trade Finance - July 2013.*

APPENDIX 2—Bank Roles in Trade Finance Transactions[8]

Banks can take the following roles in transactions covered by LOC:

- **Issuing Bank** – The bank that issues the LOC on behalf of the applicant (e.g., buyer, importer) and advises it to the beneficiary (e.g., buyer, exporter) either directly or through an advising bank. The applicant is the issuing bank's customer.

- **Confirming Bank** – Typically in the home country of the beneficiary, at the request of the issuing bank, the bank that adds its commitment to honor draws made by the beneficiary, provided the terms and conditions of the LOC are met.

- **Advising Bank** – The bank that advises the credit at the request of the issuing bank. The issuing bank sends the original credit to the advising bank for forwarding to the beneficiary. The advising bank authenticates the credit and advises it to the beneficiary. There may be more than one advising bank in a LOC transaction. The advising bank may also be a confirming bank.

- **Paying Bank** – The bank that makes payment to the beneficiary of the LOC.

- **Nominated Bank** – The bank with which the credit is available or any bank in the case of a credit available with any bank.
- **Accepting Bank** – The bank that accepts a draft, providing a draft is called for by the credit. Drafts are drawn on the accepting bank that dates and signs the instrument.
- **Discounting Bank** – The bank that discounts a draft for the beneficiary after it has been accepted by an accepting bank. The discounting bank is often the accepting bank.
- **Reimbursing Bank** – The bank authorized by the issuing bank to reimburse the paying bank submitting claims under the LOC.

[8] *Source: Federal Financial Instructions Examination Council - FFIEC BSA/AML Examination Manual – 2014*

A- INTERVIEW CONDUCTED

Mr. Steven Gruskin, HSBC Business Risk & Control Manager (BRCM) - North America BRCM Regional Head for Global Trade Finance Receivables.

B- BIBLIOGRAPHY

1) Federal Financial Institutions Examination Council - FFIEC BSA/AML Examination Manual – 2014
http://www.occ.gov/publications/publications-by-type/other-publications-reports/ffiec-bsa-aml-examination-manual.pdf

2) Financial Conduct Authority - Banks' Control of Financial Crime Risks in Trade Finance - July 2013
http://www.fca.org.uk/static/documents/thematic-reviews/tr-13-03.pdf

3) Protivity - Guide to US Anti- Money Laundering Requirements – Frequently asked questions- November 2012
http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-US-AML-Requirements-5thEdition-Protiviti.pdf

4) APG Typology Report on Trade Based Money Laundering – July 2012
http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

5) The Wolfsberg Group Trade Finance Principles (2011)
http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_Trade_Principles_Paper_II_(2011).pdf

6) Financial Action Task Force Guidance Document Best Practices Paper - Best Practices on Trade Based -Money Laundering – June 2008
http://www.fatf-gafi.org/media/fatf/documents/recommendations/

7) Financial Action Task Force – Trade Based Money Laundering – 2006
http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

8) International Chamber of Commerce
http://www.iccwbo.org/about-icc/organization/

9) Uniform Customs Code For Documentary Credits
http://www.uncitral.org/pdf/english/texts_endorsed/UCP1962_e.pdf