Transaction Monitoring in Correspondent Banking

An exploration of the unique landscape of correspondent banking and how it compares to private and corporate banking

by Amy FU Man Seung
CAMS-FCI

February 2020
# Table of Contents

1. Executive Summary ........................................................................................................... 3

2. Problem Statement and Background ................................................................................. 4

3. What Are the Three Types of Business Banking, Namely Private Banking, Corporate Banking, and Correspondent Banking? What Are Their ML Vulnerabilities and Why? .................................................. 4
   a. Definitions ....................................................................................................................... 4
   b. ML/TF Vulnerabilities and Red-Flag Indicators .............................................................. 5
   c. Similarities of Transaction Monitoring Techniques ....................................................... 8
   d. Contrast/Differences of Transaction Monitoring Techniques During Tuning, Parameters, Scenarios Setting ................................................................................................................ 10

4. Laying the Groundwork on What Correspondent Banking Is and How It Is Uniquely Situated .......................................................................................................................... 11
   a. What Are the ML Vulnerabilities of Correspondent Banking (and Why)? ...................... 11
   b. What Are the Highest Risk Elements and Red-Flag Indicators of Correspondent Banking? ... 12
   c. How to Conduct Correspondent Banking Monitoring from a Transaction Monitoring Perspective ......................................................................................................................... 13
      Qualitative Monitoring Analysis ..................................................................................... 13
      Effective TM Program, Management Cycle, and Methodology ...................................... 14

5. How Fintech/Regtech Can Assist TM in Correspondent Banking with the Advancement of Technology Innovations .................................................................................................. 20

   a. From Global Perspective, e.g., International Bodies ....................................................... 21
   b. From a Specific Jurisdiction Perspective, e.g., Hong Kong (HK) ................................... 22

7. Case Studies ......................................................................................................................... 22
   Case 1 – Westpac .................................................................................................................. 22
   Case 2 – HSBC ...................................................................................................................... 23

8. Conclusion ............................................................................................................................ 24

9. References ............................................................................................................................. 25

10. Appendices .......................................................................................................................... 28
    Appendix 1 – SWIFT Message Graphical Illustrations ....................................................... 28
    Appendix 2 – Abbreviations ............................................................................................... 30
1. Executive Summary

Used by banks throughout the world, correspondent banking services enable respondent banks to conduct business and provide services that they cannot offer otherwise (owing to the lack of an international presence and cross-border payment systems). As noted by the Financial Stability Board¹ (FSB), the ability to make and receive international payments via correspondent banking is vital for businesses and individuals, and for the international goal of strong, sustainable, and balanced growth.

However, because of the structure of this activity and the limited information available regarding the nature or purpose of the underlying transactions, correspondent banks may be exposed to money laundering and financing of terrorism (ML/FT) risks.

Anti-money laundering (AML) transaction monitoring (TM) is a preventative monitoring process used to identify potentially suspicious activity without knowing if the activity is confirmed to be fraudulent or an offence has been committed. AML transaction monitoring system (TMS) enables investigation teams to prioritise efforts in identifying suspicious activity with a higher likelihood of success, i.e., detecting fraudsters from an ocean of payments traffic. Therefore, the IT monitoring system should enable a bank to determine its own criteria for additional monitoring, filing a suspicious transaction report (STR), or taking other steps in order to minimise the ML/FT risks. This process can be operationalised by using parameters of an IT system that should allow for generation of alerts of unusual transactions, and should then be subject to further assessment by the anti-money laundering/countering financing of terrorism (AML/CFT) professionals.

In order to contribute to the common goal of AML/CFT, this paper is structured as follows: First, it raises the sceptical phenomenon on how to apply TM in different businesses: banking, namely private banking, corporate banking, and correspondent banking. Second, it identifies what their ML/TF vulnerabilities are; similarities and differences when applying TM to each specific area via TMS and management. Third, it will be more specific on TM techniques and the application of methodological approach/framework in order to achieve an effective TM program, management cycle, and methodology in correspondent banking. Next, it will explore possible solutions on how Fintech/Regtech can assist TM in correspondent banking with the advancement of technology innovations. Then, it will discuss different laws, regulations, and guidance focusing on correspondent banking compliance from a global perspective and also from a specific jurisdiction perspective, e.g., Hong Kong’s current situation. Then, two case studies on correspondent banking compliance failures in recent years will be shared so as to provide alarming signals to industry practitioners. Finally, a conclusion and some personal recommendations in response to the opening sceptical thought will be shared.

The goal of this paper is to share and shed some light on the adoption of the TM program, management cycle, and methodology in correspondent banking. Not only it could assist financial institutions (FIs) to ensure effective AML/CFT regulatory compliance, but it can also provide some insights to assist compliance professionals in banking, especially TM compliance investigators and practitioners.

---
¹ Financial Stability Board (FSB) is an international body that monitors and makes recommendations about the global financial system. It was established after the G20 London summit in April 2009 as a successor to the Financial Stability Forum (FSF). The Board members include: (a) authorities from jurisdictions responsible for maintaining financial stability, e.g., ministries of finance, central banks, and supervisory and regulatory authorities; (b) International FIs; and (c) international standard setting, regulatory, supervisory, and central bank bodies. Hosted and funded by the Bank for International Settlements, the board is based in Basel, Switzerland, https://www.fsb.org/about/
2. Problem Statement and Background

What is the best way to design a TM program for correspondent banking? Considering that each type of business banking, namely private banking, corporate banking, and correspondent banking, has its own unique business nature and financial product characteristics/features, one must not apply a one-size-fit-all approach when conducting transactions analysis and investigation during transaction monitoring for different types of business banking. By reviewing and analyzing the approach from other types of financial products/businesses banking, this paper will help hone in on how to best apply methods that are appropriate and effective for correspondent banking.

3. What Are the Three Types of Business Banking, Namely Private Banking, Corporate Banking, and Correspondent Banking? What Are Their ML Vulnerabilities and Why?

Each business banking has its own specific business nature and financial products characteristics/features that impact the transaction monitoring approach. In order to successfully prevent ML and TF, it is crucial to understand the differentiators, which not only relate to FI’s internal set-up, but also to ML/TF vulnerabilities and red-flag indicators, leading to the tailored controls and measures to be implemented relating to them. Under these connections, this section will analyse, starting from reviewing other types of financial products, discuss the unique business nature and specifics of, and then explore how to best apply methods appropriate and effective for correspondent banking.

First of all, let’s understand the definition of each type of business banking and their unique financial products characteristics/features.

a. Definitions

“Private banking (PB) is the provision of services by an FI to high net-worth individuals and where a minimum number/value of assets under management is a requirement.” The PB customer maintains a personalised relationship with the FI and receives personalised banking services, dealing, advisory, or asset/portfolio management services from the FI, and has a minimum amount, or its equivalent, in any other currency in investable assets under the FI’s management. Investable assets usually are more sophisticated financial products that comprise securities, funds, derivatives, etc. The amount may be calculated on a relationship basis covering (i) individual accounts, (ii) joint accounts with associates, and (iii) personal investment companies wholly owned by the individual or jointly owned with associates. Associate means the spouse or any child of that individual.

“Corporate banking—involves the provision of financial services such as term loans, bridging loans, ordinary credit lines, revolving credit lines, and other kinds of working capital facilities, structured finance, asset financing, and investment financing. Sometimes, it also acts as a capital and treasury market adviser for these corporate customers.” Corporate banking customers generally do not maintain a personalised relationship with the FI.

“Corresponding banking—is the provision of a current or other liability account, and related services, to another FI, including affiliates, used for the execution of third-party payments and trade finance, as well as its own cash clearing, liquidity management and short-term borrowing or investment needs in a particular currency.” Corresponding banking customers generally do not maintain a personalised relationship with the FI.

---

2 The Wolfsberg, Correspondent Banking Due Diligence Questionnaire (CBDDQ) Glossary, 22 February, 2018
4 Hong Kong Institute of Bankers, Banking Industry Commercial / Corporate Banking Specification of Competency Standards, May 2013
5 The Wolfsberg, Anti-Money Laundering Principles for Correspondent Banking, 2014
Some of the different specifics of three types of business banking in the table below (non-exhaustive list):

<table>
<thead>
<tr>
<th>Financial Products Characteristics/Features</th>
<th>Private Banking</th>
<th>Corporate Banking</th>
<th>Correspondent Banking</th>
</tr>
</thead>
<tbody>
<tr>
<td>i) Financial amount/value per transaction</td>
<td>Usually large in value</td>
<td>Medium to large, depends on corporate size</td>
<td>Depends on the FI size and scale</td>
</tr>
<tr>
<td>ii) Frequency/volume of transactions per period</td>
<td>Usually infrequent</td>
<td>Depends on corporate size and usage</td>
<td>Depends on the FI size and scale</td>
</tr>
<tr>
<td>iii) Sophistication of products structure</td>
<td>Usually complex</td>
<td>Traditional trade financing products</td>
<td>Payments traffic/fund transfers only</td>
</tr>
<tr>
<td>iv) Sophistication of clientele background</td>
<td>Usually sophisticated</td>
<td>Depends on corporate size</td>
<td>Mostly large institutions or FIs</td>
</tr>
<tr>
<td>v) Customer servicing mode/approach</td>
<td>Personalised relationship serviced by defined relationship manager</td>
<td>Normally serviced by FI’s corporate team</td>
<td>Normally serviced by FI’s institutional business team</td>
</tr>
</tbody>
</table>

b. ML/TF Vulnerabilities and Red-Flag Indicators

Recognising where ML/TF vulnerabilities posed by various banking businesses and their financial products, FIs can adopt appropriate approaches, implement proper controls and measures, and enhance their ability to mitigate and manage related ML/TF risks.

*Private Banking Vulnerabilities*°

Private banking can be vulnerable to ML/TF due to the availability of bespoke product features tailored to a client’s needs, complex products and services offered in a relatively secured banking environment, and usually involving high-value transactions. The following factors contribute to the increased vulnerability of PB business.

- Wealthy and powerful clients—PB clients may be reluctant or unwilling to provide adequate documents, details, and explanations, especially if the client enjoys a high public profile where the client may exert political or economic power or influence. The close relationship developed by PB bankers with their clients may also blur the conflict of interests’ alertness.
- Multiple and complex accounts—PB clients often have many accounts in more than one jurisdiction, either within the same FI or FI group, or with different FIs. Thus, regarding an individual FI, it is more difficult to assess the true purpose and business rationale for individual transactions.
- Concealment and confidentiality—Most PB clients seek confidentiality regarding their beneficial ownership and/or that the business services requested be handled anonymously. By using offshore trusts and/or involving complex structures, such as private investment companies (PICs), shell companies help to achieve some extent of secrecy about the beneficial ownership of assets/funds.
- Offshore tax havens—Certain jurisdictions have promoted their low service-fee charges and/or zero tax rate over business income supported by their legislation, despite international bodies encouraging legalisation of beneficial ownership transparency.
- Countries where corruption is notorious or perceived to be a common source of wealth/business income.

*Red-Flag Indicators*

- Movement of funds—The transmission of funds and other assets by private clients often involve high-value transactions, requiring rapid transfers to be made across accounts in different countries and regions of the world.

• Usage of concentration accounts—Multi-client pooled/omnibus type accounts used to collect together funds from a variety of sources for onward transmission are seen as a potential major risk.
• Credit—The extension of credit to clients who use their assets as collateral also poses a money-laundering risk unless the lender is satisfied that the origin and source of the underlying asset is legitimate.
• Commercial activity—Activity is conducted through a personal account, or personal activity is conducted through a business account so as to deceive the FI or its staff.

Corporate Banking Vulnerabilities

Corporate banking deals with a wide spectrum of corporate customers, from local small stores to international corporations with offices across the world. One of the risks specific to this sector is the trade-based money laundering (TBML) process, which has been recognised by the Financial Action Task Force (FATF) in its 2006 study as one of the main methods by which criminal organisations and terrorist financiers move/conceal their profits derived from illegal activities. The international trade system might be easily exploited by launderers and terrorist financiers due to the enormous volume of trade flows, complexity of foreign exchange transactions, and mixing illicit and legitimate funds. Moreover, it is extremely difficult for an FI to verify whether the actual exchange of goods or services took place, or whether it was just fake-invoiced because each FI alone is just a piecemeal of the entire trade transaction cycle for goods and services traded from seller to buyer.

While there is no exhaustive list of trade-related products and services, some indicative examples of products or services that typically fall within the scope of “trade finance” services provided by banks include:

- Bank guarantees
- Documentary collections
- Financing under open account transactions
- Forfaiting and risk participation
- Import/export loans
- Packing loans
- Pre-shipment loans
- Structured trade financing
- Trust receipts
- Warehouse financing
- Import/export invoice discounting
- Letters of credit (L/C)
- Financing for transactions under L/Cs

The following are common indicators easily abused by ML/TF via TBML:

Topologies
- Over-/Under-invoicing
- Over-/Short/Phantom shipping
- Fictitious trades
- Use of shell or fictitious companies
- Multiple-invoicing of goods and services
- Black market trades

Red-Flag Indicators

1) Discrepancies appear between the description of commodity traded on the bill of lading and payment order or invoice, e.g., inconsistency in the product amount or type.
2) Significant discrepancies appear between the pricing or the value of the product or service reported on the invoice and its fair market value (undervalued or overvalued).
3) The method of payment appears inconsistent with the risk characteristics of the transaction, e.g., the use of an advance payment for a new supplier in a high-risk jurisdiction.
4) A transaction involves the use of letters of credits that are amended, extended, or change payment location frequently or significantly without a reasonable explanation.

---

7 Anna Piwowarska, AML Transaction Monitoring Overview: Banking segments differentiators - Retail, Corporate, Correspondent and Investment Banking, 8 February 2019
8 HK Association of Banks, Guidance Paper on Combating TBML, p.2-3, 1 February 2016
5) Letters of credit, negotiable instruments, or other means are used that are issued overseas without trade basis to obtain financing.

6) Commodities shipped are inconsistent with the customer’s industry or operations, or are unrelated to the customer’s business nature.

7) Customers are involved in high-risk suspicious ML/TF activities, including importing/exporting goods that are subject to embargo or restrictions (e.g., military supplies of foreign governments, weapons, chemicals, or natural resources, e.g., metals).

8) The commodity includes dual-use goods.

9) The commodity is shipped to or from high ML/TF risk jurisdictions.

10) The type of commodity shipped is vulnerable to ML/TF, e.g., high-value but low-volume goods (e.g., diamonds, precious metals, and artworks).

**Correspondent Banking Vulnerabilities**

**Correspondent banking**\(^{10}\) relationships are essential for the effectiveness of the global financial network, however, they are vulnerable to exploitation by criminals due to their scale, complexity, and level of anonymity. Transaction monitoring controls are required from respondent and correspondent banks, but with limited know your customer (KYC) information available on the respondent bank’s clients, the efficiency of such controls might thus be compromised from a correspondent bank perspective.

A correspondent bank can request information from respondent, however, given the number of alerts generated every day and limited resources available, the full picture of the alerted activity is blurred and hard to assess. The matter gets only more complicated when nested correspondence relationships are used—more layers of intermediaries can leave the money trail obscure and difficult to decipher. Quite often, correspondent services are offered to non-banking FIs, such as money remitters, which, due to their limited customer identification procedures, should be accompanied by more scrutiny when monitoring movement of funds.

The following are common indicators of funds transfers/bank-to-bank transactions:

**Red-Flag Indicators**\(^{11}\)

1) The size and frequency of currency deposits increases rapidly with no corresponding increase in non-currency deposits.

2) A bank is unable to track the true account holder of correspondent or concentration account transactions.

3) The turnover in large-denomination bills is significant and appears uncharacteristic given the bank’s location.

4) Changes in currency-shipment patterns between correspondent banks are significant.

5) Many funds transfers are sent in large, round-dollar, hundred-/thousand-dollar amounts.

6) Funds transfer activity occurs to or from a financial secrecy haven, or to or from a higher-risk geographic location without an apparent business reason, or when the activity is inconsistent with the FI counterparties’ business or history.

7) Many small, incoming transfers of funds are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the FI counterparties’ business or history.

8) Large, incoming funds transfers are received on behalf of a foreign FI counterparty, with little or no explicit reason.

9) Funds transfer activity is unexplained, repetitive, or shows unusual patterns.

10) Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.

11) Funds transfers are sent or received from the same person to or from different accounts.

12) Funds transfers contain limited content and lack related party information.

13) Funds transfers involve shell banks and/or banks offered payable-through accounts.

---

\(^{10}\) Same as footnote 7 above.

c. Similarities of Transaction Monitoring Techniques

Despite illustrating the vulnerabilities and red-flag indicators relating to the three types of banking businesses above, when facing the increasing demands/drivers from regulatory expectations/requirements on stronger compliance risk management, converging compliance risks, and controls processes, gaining consistent view of compliance risks enterprise-wide, etc., FIs’ transactions pattern monitoring technique shares some common principles/framework:

1) Stemming from effective AML/CFT governance/framework:

A successful and good transaction monitoring system commences from an effective AML/CFT governance/framework of the bank. It is because each step is closely linked and interconnected to the next steps, which starts from these:

i. KYC/CDD data should be correctly obtained by frontline.

ii. Effective and adequate AML/CFT policies and procedures should be in place so that proper guidance provided to staff.

iii. Data quality should be correctly captured in the bank’s customer database upon obtainment from customers.

iv. Sanctions compliance depends on effective sanctions screening system management maintained with the timely update of designated parties database upon customers data quality assured/captured.

v. Effective transaction monitoring system depends on properly established customer profiles using risk-based approach (RBA), good knowledge and understanding of clientele nature, and anticipated business activities (taken into account the size, nature, and complexity of the bank’s overall business, products, and services, etc.), optimised and justified rules and thresholds/parameters setting of scenarios for proper application of differentiated monitoring for customers with different levels of ML/FT risks, and assistance to identify suspicion, e.g. when transaction activity is incommensurate with the customer’s profile or income, etc.

vi. Effective transaction monitoring also depends on appropriate handling and management of pre-transaction screening alerts clearance, post-transaction pattern monitoring alerts clearance, proper documentation of alerts investigated, and timely filed suspicious transaction reporting (STR) if necessary.

vii. Effective ongoing monitoring depends on periodically reviewing customer profiles in accordance with different risk classification, transaction monitoring system, and sanctions screening system to ensure they remain optimal for the bank and address ML/TF risks, taking into account changes and developments in business operations and ever-changing ML/TF methods.

2) Transactions monitoring rules/scenarios setting:

Suspicious rules/scenarios, no matter the different banking businesses, typically build around red-flag indicators and include transactions conducted with:

i. High-risk jurisdictions

ii. Large transaction amount/value

iii. Rapid movement of funds

iv. High-risk customers

v. Change in behaviours/volume with external party

vi. Change in behaviours/volume with internal customers

vii. Change in behaviours/volume with customer itself
In designing transaction monitoring systems and processes, including setting of parameters and thresholds, an FI can take into account transactions characteristics, which may include:

a. nature and type of transactions (e.g., abnormal size or frequency),
b. nature of a series of transactions (e.g., structuring a single transaction into a number of cash deposits),
c. counterparties of transactions,
d. geographical origin/destination of a payment or receipt, and
e. customer’s normal account activity or turnover.

3) Relationship-based transaction monitoring:

By adopting risk-based approach, banks should ensure that transaction monitoring carried out by way of relationship-based or the overall relationship/customer, rather than on an individual account basis.

For example, it is advisable that the FI should ensure the transaction monitoring systems and processes can support the ongoing monitoring of a business relationship in a “holistic approach,” which may include monitoring activities of a customer’s multiple accounts within or across lines of businesses, and related customers’ accounts within or across lines of businesses. This means an FI preferably adopts a relationship-based approach rather than on a transaction-by-transaction basis.

Relevant indicators of business relationship

- All related account numbers and group numbers (where applicable)
- Purpose and intended nature of related accounts
- Anticipated level and nature of the activity that is to be undertaken through the relationship (e.g., the typical transactions are likely to be as provided by customer)
- Origin/destination of the funds
- Banking history

Transactions-based relationship indicators

- Reviewing periods of fund flows
- Previous transactions pattern (e.g., dormant)
- Total amount of deposits and withdrawals
- Counterparties information
- Suspicious indicators and patterns (e.g., frequent transactions/large-amount transactions)

4) Application of intelligent machine learning capability of transaction monitoring system

Once the automated transaction monitoring system is installed, it is suggested to apply the intelligent machine learning functionality (a.k.a. suppression of alerts) that offers deeper insights, reduces false positives, and renders the whole post-transaction monitoring process more efficient.

However, the suppression logic should be appropriately applied for low- and medium-risk levels of customers, and those suppressed alerts should be generated for review again upon a predefined number of times suppressed, e.g., three or five times according to the risk tolerance level of each FI.

---

12 Hong Kong Monetary Authority, Guideline on AML/CFT (For Authorized Institutions), s.5.7, Revised Oct 2018
13 Hong Kong Monetary Authority, Guideline on AML/CFT (For Authorized Institutions), s.5.6, Revised Oct 2018
14 Hong Kong Monetary Authority, Guidance Paper on Transaction Monitoring, Transaction Screening and Suspicious Transaction Reporting, p.14 to 15, Revised May 2018
15 Same as footnote 14 above
16 Umberto Lucchetti Junior, AML Rule Tuning: Applying Statistical and RBA to Achieve Higher Alert Efficiency, ACAMS White paper
d. Contrast/Differences of Transaction Monitoring Techniques During Tuning, Parameters, Scenarios Setting

1) “Parameter/thresholds” setting based on specific bank’s clientele profiles:

“Parameters/thresholds” setting should be built based on each bank business nature, characteristics, and segments/sub-groups of clientele, i.e., there is no one-size-fit-all universal thresholds/benchmarks, even between the same industry peers/FIs.

2) Some “rules/scenarios” setting for overall business line/bank-wide clientele for comparison:

Suspicion could also be established for unjustified large (reportable) amounts, sudden and/or significant changes in transaction activity by value or volume (i.e., frequency), etc., within the same business line (for large FIs) or within the same bank (for small FIs) when compared with the overall business line/bank-wide clientele base, besides monitoring alerts established for specific business banking clientele segments/sub-groups (i.e., point 3.d.1 above).

3) Monitoring for intra-customer (i.e., customer itself) transaction activities/pattern comparison:

i. **Private banking:** This type of business segment basically serves the banking and investment purposes of relatively larger amount/value for HNWIs, which requires for more a “closely and tailored” servicing relationship. To some extent, as a result, their transactional activities (i.e., fund transfers) are presumed/deemed for HNWIs’:
   a. “personal investments only,” i.e., not intended with third parties’ transactions; or
   b. not for daily personal expenses (which should be under retail banking business segment); or
   c. not intended to comingle between the HNWI’s personal account with his/her external business-related company account for operational purpose, even under the same UBO(s) to avoid the suspicion of tax evasion.

Therefore, in some instances where applicable, the sources/destination of funds of the transactions, the source of wealth of the HNWIs and their connected accounts or relationships would be important sources of information for providing detailed background about the suspicion for transaction monitoring analysts when conducting investigation.

ii. **Corporate banking:** presumably reasonable transactions with third parties. This type of business segment basically serves the corporate financing purpose or business transactional relationship between buyer and seller due to international trade finance transactions. Thus, it is normal to find fund transfers with third parties’ transactions. Therefore, the purpose and intended nature of the account usage as provided by the customer are important to be justifiable and commensurate with the “anticipated account activities” to ensure consistency.

However, alertness should still be maintained: If any advantage is being taken to comingle fund transfers/transaction activities between the customer and any unknown third parties, or if the customer account is being used for its business operational daily cash management purpose to avoid suspicion of tax evasion.
iii. **Correspondent banking**: Used by banks throughout the world, correspondent banking services enable respondent banks to conduct business and provide services that they cannot offer otherwise (owing to the lack of an international presence and cross-border payment systems).

Because of the completely different purpose and structure of correspondent banking activity and the limited information available regarding the nature or purpose of the underlying transactions, correspondent banks may be exposed to ML/FT risks. However, there are no such “underlying transaction” or “correspondent/intermediary/respondent bank” relationship when compared with private banking and corporate banking. As such, the transaction monitoring technique for correspondent banking is a totally different picture, which will be discussed in more details in the next section.

4. Laying the Groundwork on What Correspondent Banking Is and How It Is Uniquely Situated

a. What Are the ML Vulnerabilities of Correspondent Banking (and Why)?

Correspondent banking is an arrangement under which one bank (correspondent) holds deposits owned by other banks (respondents) and provides payment and other services to those respondent banks. Such arrangements may also be known as *agency relationships* in some domestic contexts. In international banking, balances held for a foreign respondent bank may be used to settle foreign exchange transactions (Example 1). Reciprocal correspondent banking relationships may involve the use of so-called nostro and vostro accounts to settle foreign exchange transactions (Example 2).

**Example 1**

The correspondent often has no direct relationship with the underlying parties to a transaction and is therefore not in a position to verify their identities. In essence, correspondent banking is a non-face-to-face business segment. Even more dangerous, potentially and theoretically, the respondents could allow its respondents to

---

17 BCBS, *Guideline on Sound management of risks related to money laundering and financing of terrorism* Annex 2 Correspondent Banking, p.23, June 2017
18 From footnote 43 of footnote 17 above. i.e. Such as “cash management (e.g., interest-bearing accounts in a variety of currencies), international wire transfers, cheque clearing, payable-through accounts, and foreign exchange services,” FATF Glossary in the FATF recommendations.
19 BIS, *Correspondent Banking*, p.43, July 2016, CPMI
further use by its customers/respondents, i.e., unlimited “nested” correspondent relations. Thus, this business segment should be regarded as high risk from a ML and/or TF perspective, despite that, since 2015, regulators and supranational AML supervisory bodies are recognising the growing threat posed by lax AML controls, not only to smaller banks and non-banks, but also to some big banks.

Therefore, correspondent banking relationships, if poorly controlled, can allow other FIs with inadequate AML/CTF systems and controls, and customers of those FIs, direct access to international banking systems.

b. What Are the Highest Risk Elements and Red-Flag Indicators of Correspondent Banking?

**Highest-Risk Respondents**

Any correspondents are those that:

- are offshore banks limited to conducting business with non-residents or in non-local currency, provide banking services that will be used, via payable-through-account(s) activity, by either the respondent bank’s affiliates (nested correspondent banking) or other third parties, and are not subject to robust supervision of their AML/CTF controls;
- are domiciled in jurisdictions with weak regulatory/AML/CTF controls or other significant reputational risk factors, e.g., corruption; or
- are shell banks or any respondent which provides banking services to shell banks.

**Red-Flag Indicators**

- The amount of credits and debits in an account held by an FI is apparently inconsistent with its scale of depositor nature of business, or the fluctuations of credits and debits in such account apparently exceeds the fluctuation of its deposits.
- The actual accountholder of a payable-through account is not identifiable.
- The currency-shipment patterns with a respondent bank has a significant change.
- A respondent bank rapidly increases the amount and number of cash deposits while its non-cash deposits are not relatively increased.

---


25 Reference Source: Qatar Financial Centre Regulatory Authority, *Guidance on Correspondent Banking Services*, Figure 1, May 2018

c. How to Conduct Correspondent Banking Monitoring from a Transaction Monitoring Perspective

Qualitative Monitoring Analysis²⁷

The level of monitoring activity undertaken by a correspondent on its respondent’s activity should be commensurate with the risks posed by the respondent. Due to the significant volume that correspondent banking activity can entail, together with the need to work within prescribed scheme settlement deadlines, electronic and/or post-execution monitoring processes are often the industry practice. The following possible techniques of monitoring activity combine to represent electronic-monitoring good practice in the area of correspondent banking relationships:

1) Anomalies in behaviour
   Monitoring for sudden and/or significant changes in transaction activity by value or volume

2) Hidden relationships
   Monitoring for activity between accounts and customers (including respondents and their underlying customers). Identify common beneficiaries and remitters or both among apparently unconnected accounts/respondents. This is commonly known as link analysis.

3) High-risk geographies and entities
   Monitoring for significant increases of activity or consistently high levels of activity with (to or from) higher-risk geographies and/or entities.

4) Other money laundering behaviours
   Monitoring for activity that may, in the absence of other explanation, indicate possible money laundering, such as the structuring of transactions under reporting thresholds or transactions in round amounts.

5) Other considerations
   In addition to the monitoring techniques above, the monitoring system employed to monitor correspondent banking for AML/CTF purposes should facilitate the ability to apply different thresholds against customers that are appropriate to their particular risk level.

6) Ongoing monitoring of correspondent banking relationships
   In addition to monitoring account/transaction activity, a correspondent should monitor a respondent for changes in its nature and status. As such, information about the respondent collected during the customer acceptance and due diligence processes must be:
   - reviewed and updated on a periodic basis (periodic review of FI customers will occur on a risk-assessed basis); or
   - reviewed on an ad hoc basis as a result of changes to the FI customers’ information identified during normal business practices; or
   - reviewed when external factors result in a material change in the risk profile of the FI customer.

Where such changes are identified, the respondent should be subject to a revised risk assessment and a revision of their risk classification, as appropriate. Where, as a result of the review, the risk classification is altered (either up or down) an FI should ensure that the due diligence standards for the respondent’s new risk classification are complied with and timely updated. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk level.

²⁷ Same as footnote 24 above, p154-155.
FI s should consider terminating the accounts of respondents and consider their obligation to report suspicious activity for respondents who fail to provide satisfactory answers to reasonable questions regarding transactions/activity passing through the correspondent relationship, including, where appropriate, the identity of their customers (i.e., FI customer’s customer) featuring in unusual or suspicious transactions or activities.

In summary, increasing costs, regulatory requirements and an increased perception of risk are reducing the profit margins associated with this CBR activity in some countries and/or with some FI customers, and could be making this business line increasingly unappealing to a growing number of correspondent banks. In particular, CBR is a business highly influenced by economies of scale, where banks are struggling to make returns when the business volumes in certain jurisdictions and/or with certain customers are not considered to justify the compliance costs involved. The perception is that this business line has shifted from being a low-risk/low-margin segment to a high-risk/low-margin one.

From the regulatory side, no significant changes in AML/CFT have been introduced recently, and banks are expected to continue applying a risk-based approach for their customer due diligence in relation to AML/CFT. There are indications, however, that in some instances the perception of the ML/FT risks associated with activities, such as correspondent banking, is changing. The term “de-risking” is commonly used to refer to those instances in which banks adopt “increasingly stringent financial crime–related policies to reduce their exposure to potential money-laundering, terrorist-financing, corruption, and sanctions risks.”

Effective TM Program, Management Cycle, and Methodology

In order to ensure proper application and effective TM and management for correspondent banking relationships, the following procedural cycle and each process’s specific techniques could be applicable guidance for industry practitioners, e.g., transaction monitoring/investigation team of FIs.

From a correspondent banking perspective, the seven essential components of transaction monitoring methodology/program include:

1) FI counterparty segmentation
2) Anomaly activities/behaviours profiling
3) Scenarios setting
4) Tuning optimal thresholds values/parameters to scenarios setting
5) Ongoing tuning of optimal thresholds values and suspicious TM scenarios
6) Ongoing TM of correspondent bank relationships
7) Ongoing TM of non-customer correspondent bank relationships

1. FI Counterparty Segmentation

First and foremost, the fundamental component of an effective TMS should be based on a clear and comprehensive picture of different counterparty types with which a bank has a business relationship. This process forms the backbone of TM and is concerned with the groupings of FI counterparties based on similar business attributes and transactional behaviour. Segmentation, when done well, enables AML typologies to focus on unusual behaviours for specific groups of FI counterparties, using threshold values (more details in step 4 below) that allow precise detection of bad actors while minimising the number of false positive alerts. Different types of FI counterparties may be categorised by:

- With/without RMA
- Customer/non-customer
- Affiliate/non-affiliate
- Domestic/foreign

In the face of a large amount of transactional activities data, different groups of FI counterparties can be segmented based on transactional activity and behaviour. The population data can be segmented by applying

---

14

---

28 Same as footnote 19 above, p.12.
29 Same as footnote 19 above, footnote 8.
a top-down approach and a bottom-up approach. Using the top-down approach, based on business knowledge, FI counterparties can be initially characterised based on known attributes. The bottom-up approach, which is a data-driven process by common statistical methods—e.g., mean, median, skewness, kurtosis, coefficient of variation, and the empirical percentile distribution—can be used to identify homogenous customer groups with similar transactional behaviours.

Keep in mind that inaccurate segmentation with large, uneven groups may lead to high alert volumes with a high level of noise (false positives), giving rise to the inefficient use of investigator effort and resources that ruins the later/overall TM processes.

Besides proper segmentation, equal importance is the requirement of “data quality” captured in the FI’s KYC/CDD database and systems (DNS). KYC Registry and Bankers Almanac could be industry reference sources.

2. Anomaly Activities/Behaviours Profiling

An effective TM of counterparties also depends on a sound knowledge of what types of counterparty transaction activities and message traffic are to be monitored. This requires some understanding of AML topologies of CBRs, i.e., what constitutes transactional red flags/risk indicators, or attributes and funds transfer operational knowledge, for example.

**High-Risk Attributes of Counterparty FIs (non-exhaustive list)**

- Country and/or region
- Transaction amount/period (average or total)
- Transaction volume/period (average or total)
- Currency involved
- Business types/areas, e.g., private or commercial or retail banking
- Types of counterparties, e.g., domestic and/or foreign
- Counterparty risk level, e.g., PEPs involved in senior management of FI/adverse negative news related to ML/TF
- Types of products and services offering, e.g., payable through accounts (PTAs)/holdmail/trade finance/MSB or MVTS/downstream or nested relationships, etc.

**SWIFT30 Message Types** (see Appendix 1)

- MT 103
- MT 202 and MT 202COV
- MT 205 and MT 205COV

Each risk attribute would be properly risk-scored by a risk-based approach (RBA). Upon identifying various risk attributes together with end-to-end payment flows information, transactional activity profiling/metrics could be constructed. The process flow follows a top-down approach33 as follows:

---

30 SWIFT provides a network that enables FIs worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment.

31 SWIFT Message Type Reference: https://docs.oracle.com/cd/E19509-01/820-7113/6nidSdl2r/index.html


33 Reference source: SWIFT, Compliance Correspondent Monitoring, Factsheet, Mar 2017
3. Scenarios Setting

Based on the roles of FI counterparties involved and highest-risk payments flows identified, suspicious activity scenarios/rules could be developed focusing on “targeted/suspected” transactional activities:

- High-risk attributes – e.g., counterparty (foreign correspondents or offering PTAs or DCS\textsuperscript{34}), countries
- High-risk/suspicious transaction pattern – see below in more details
- Change in behaviour – transaction amount/volume over certain period (e.g., compared with average of previous month, last 12 or 24 months, etc.)

Analysis of incoming/outgoing transactions, i.e., payment flows direction and the role of FI counterparty, are also important information to assist end-to-end transaction flow investigation. Role of FI counterparty in fund transfer/payment chain may be:

Example: Basic MT103 Message Flow\textsuperscript{35}

<table>
<thead>
<tr>
<th>Inbound/Incoming Flows:</th>
<th>Outbound/Outgoing Flows:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Counterparty FI Role</strong></td>
<td><strong>My Role</strong></td>
</tr>
<tr>
<td>Originator</td>
<td>Beneficiary</td>
</tr>
<tr>
<td>Intermediary</td>
<td>Beneficiary</td>
</tr>
<tr>
<td>Originator</td>
<td>Intermediary</td>
</tr>
<tr>
<td>Intermediary</td>
<td>Intermediary</td>
</tr>
</tbody>
</table>

\textsuperscript{34} FFIEC Bank Secrecy Act/AML InfoBase: Correspondent Accounts (Domestic): https://bsaaml.ffiec.gov/manual/ProductsAndServices/01

Red-Flag Indicators of Correspondent Banking Transactions Pattern/Scenarios\(^{36}\) (non-exhaustive list)

1) High volume in round amount
2) Multiple routing
3) U-turn transaction
4) Potential structuring
5) Potential misuse of MT202

Suspicious Rationale and Examples:

**Red-Flag Indicators #1 and #2**

1) Large number of wire transfers for large round-dollar amounts
2) Large number of wire transfers to/from unrelated third parties

**Red-Flag Indicators #3 or #4**

1) A large incoming wire transaction followed by numerous smaller outgoing wire transactions
2) Numerous small wire transfers from the same correspondents that maintain a low balance
3) Unexplained, sudden numerous wire transfers, especially inconsistent with past historical pattern

**Red-Flag Indicator #5 – Potential Misuse of MT 202**

“If the originating bank does not flag the MT 202 message as a cover message when using the MT 202 COV—perhaps as a result of technical problems or even with fraudulent intent—the other banks in the payment chain will not receive all relevant information. Moreover, since an MT 202 payment without the cover indicator is a simple interbank payment, the intermediary banks will accept the MT 202 and be unaware that relevant information is missing. Therefore, the risk exists that a bank could unknowingly accept a message without complete information. In particular, the intermediary bank, which without the information of originator and beneficiary due to not its customer by nature, might not be able to fulfil its regulatory obligations.

Moreover, it needs to be acknowledged that if banks that have the intention to engage in deceptive practices, it is almost impossible for correspondent banks, especially for intermediary institutions, to detect this—irrespective of the method used. For instance, a bank that deliberately chooses the MT 202 instead of the MT 202 COV in order to avoid including additional information about the transaction.”\(^{37}\)

In addition, “monitoring the potential misuse of the MT 202 message type is difficult because the amount of MT 202 message traffic which contains non-FI third parties appearing to be related to trade finance transactions, such as letter of credits. There seems to be a consensus that non-FI third parties can be involved in a “cover payment” via the MT 202 and MT 103 message streams/pair if the transaction is a letter of credit as this would be considered an interbank transfer.”\(^{38}\)

\(^{36}\) Same as footnote 35 above

\(^{37}\) BIS, Committee on Payments and Market Infrastructures, Correspondent Banking, p.36, 38, July 2016

\(^{38}\) Keith Furst, How the misuse of SWIFT MT 202 is fuelling financial crime, Online: https://www.greshamtech.com/blog/swift-mt-202-misuse-financial-crime, 5 April 2016
Because of the above, transaction monitoring scenarios should be set to avoid these “targeted/suspected” correspondent activities, no matter whether structured by criminals deceptively or unknowingly facilitated by intermediary banks, in order to:

- identify and review large or unusual transactions to determine their nature as to whether they are consistent with the nature of the customer’s business, customer base, or market; and
- analyse transactions to identify behaviours indicative of nested accounts, intermediary, or clearing agent services, or other services for third-party foreign FIs that have not been clearly identified.

4. **Tuning Optimal Thresholds Values/Parameters to Scenarios Setting**

Within customer segmentation in step 1 above, the initial threshold values/parameters have been established by business logic. By applying these initial threshold values to the scenario setting in step 3, the next step is to tune the thresholds values in order to optimise the most applicable parameters from the FI’s counterparties transaction activities to improve alert generation quality.

An effective tuning process can apply analytical approach by “above/below the line” testing method (ATL/BTL)\(^{39}\). In this step, the (initial) threshold values can be adjusted in a tuning environment, and an alert generation cycle is tried such that the alerts can be reviewed by investigators and compared with red flags and SARs filed. Adjustments to thresholds can be made using statistical analysis of counterparties transactions, moving them above or below pre-determined multiples of standard deviation.

Then, UAT investigations, i.e., model validation should be performed. During this step, a thorough investigation of alerts generated in a testing (UAT) environment allows investigators/compliance team to assess the alerts being generated by the scenarios setting in step 3 above. The influential factors include: ratio of good versus bad alerts, data availability, alerts volume, and human resource availability. Additionally, if SARs data is available, e.g., ratio of alert-to-SARs and the nature of SARs could enhance the tuning UAT for evaluating alerts before putting into production.

Up until this stage, a risk-based and effective TM methodology is formed for correspondent banking/FI counterparties. Having said, the same analytical and statistical TM methodology could be applied in any line of business, business banking, customer segments, etc.

5. **Ongoing Tuning of Optimal Thresholds Values and Suspicious TM Scenarios**

There are always new trends and ML schemes as time evolves. ML criminals would become more sophisticated and change different means, values/amounts, i.e., tactics to seek compliance loopholes in order to circumvent FI’s AML control measures. As such, compliance professionals and investigations team should:

- keep abreast of new schemes and regulatory requirements, e.g., periodic typology reports and publication released by international AML/CFT organisations;
- assess any monitoring gaps that exist and devise plans to create new scenarios or fine tune existing rules continuously; and
- maintain a close link with business teams to understand any new business trends, products, or services that will be offered by FI counterparties in order to reassess risk and mitigate them with updated/tuned scenarios.

6. **Ongoing TM of Correspondent Bank Relationships**

Correspondent accounts are, in essence, as mentioned in section 3.2.a above, bank accounts, non-face-to-face business by nature, and the correspondents have limited knowledge about the “underlying transaction” and must be therefore a high ML/TF risk business and subject to the same mandatory AML/CFT transaction monitoring. However, an actual situation is not the same. It is far more difficult and requires a different approach because\(^{40}\):

---

\(^{39}\) Protiviti, White paper on *Tuning Suspicious Transaction Monitoring Scenarios: Combining AML Expertise and Data Analytics*, 2013

The information retained in the SWIFT message may sometimes be incomplete and/or misleading. As mentioned in section 3.2.d step 3 under “Red-Flag Indicator #5 – Potential Misuse of MT202” (under Suspicious Rationale) the correspondent does not know the FI counterparty’s nested correspondent relation, where the underlying transaction originated from.

The individual amounts may be huge, and/or the number of the transactions may be huge. Upon “urgent” situation, e.g., when “cut-off time” is approaching, but a huge volume of transactions is being handled, alertness between suspicious and ordinary easily becomes blurred. Thus, the correspondent may have just “accepted” or “passed on” the transaction details to the next FI counterparty.

How do you monitor transactions when your bank/FI, e.g., being an intermediary bank/FI (i.e., sending/receiving correspondent), does not have insight into the source of funds (originating customer) or destination of funds (beneficiary customer), and when the transactions are in fact not your customers’ transactions? Illustrative example:

The suspicions or baseline follow the same set of rules: high-risk jurisdictions, unjustified large amounts, structuring, threshold monitoring, sudden and/or significant changes in transaction activity by value or volume, etc.

If in doubt, request for information from your FI counterparty until one is satisfied with the reasonableness because TM is a mandatory responsibility of each bank.

7. Ongoing TM of Non-Customers Corresponding Bank Relationships

Despite Wolfsberg providing some suggested procedures (e.g., monitoring by volumes and/or message types, and significant changes in usage or cancellation due to compliance reasons) for ongoing TM of non-customer FI counterparties, unlike a bank’s own customers for which KYC information is available, very little is known about non-customer FIs. Because a definite identification of the party does not exist, it is particularly difficult to monitor these non-customer CBRs.

In order to capture the non-customers’ transactional behaviour, an exhaustive list of features needs to be created in order to uncover the hidden behaviour and reflect the AML risks. Since segmentation is the fundamental component of the AML TM process, the suggested approach should stem from the very beginning, i.e., proper segmentation which includes three parts:

1. Feature Expansion – The list of features is expanded vertically and horizontally to reflect as many AML risks as possible. This is done vertically by expanding past transaction volume and the dollar amount to include transaction/message types, with currency and trend data on various intervals. Horizontally, by

---

41 Reference source same as footnote 40 above.
43 The Wolfsberg Group, Guidance on SWIFT Relationship Management Application (RMA) Due Diligence, p.3 2016
looking at counterparties’ information in greater detail, it is expected that increasing the number of considered features could drive the performance improvements (reduction in false positives volume).

2. *Machine Learning*[^44] – By using more features in SWIFT message data to segment customers based on customers and transactions, including transactional data (type, direction, value, originator, date), customer data (geographical, chronological), and risk data to create segments for analysis—and then applying objective machine learning to create the most refined and up-to-date segments possible. The crucial difference is that by assigns—and reassigns—of non-customers to segments based on their actual behaviour, revealed in their real transactions and true interrelationships, over time.

3. Once the optimal group structure is identified, a decision tree model can be created, and then the distribution of non-customers within the groups be evaluated. This validates the resulting thresholds and scenarios objectively and can be applicable to the bank’s existing TMS.

Based on the above, implementing and improving AML detection in correspondent banking, even for non-customers’ correspondent banking relationships, becomes feasible and achievable by applying the seven essential components of transaction monitoring methodology/framework for CBRs.

5. How Fintech/Regtech Can Assist TM in Correspondent Banking with the Advancement of Technology Innovations

As suggested by the Institute of International Finance (IIF) in 2017[^45], several technologies are or may in the future contribute to Regtech solutions in AML/CFT:

1. **“Big data” infrastructure:** by unlocking information across the organisation: applying big data technologies to AML/CFT investigations. Such data include transactions metadata, client information on proprietary systems, information from external sources, including “deep web threat intelligence,” public sources, and KYC utilities.

2. **Artificial intelligence/Machine learning:** improved analytical capabilities through its ability to apply detection rules to vast volumes of data, identify complex patterns and non-linear relationships, and analyse unstructured data sources. When applied to transactions and account monitoring, it can detect suspicious activity more accurately.

3. **Robotics:** the use of artificial intelligence (AI) to automate manual tasks, managing processes related to AML/KYC investigations.

4. **Shared utilities:** could in the future be applied to AML/KYC information storage and sharing among FIs and FIUs. Today, KYC/AML information is stored in FI organisational silos behind confidential information barriers, requiring the creation of centralised intermediaries to gain efficiencies across the market.

5. **Biometrics:** through the application of biometrics. An FI can ascertain an (onboarding) customer’s identity through biometrics remotely, rather than requiring the customer to visit a bank branch to establish his identity by handing over official identification documentation.


Key Solutions for AML/CFT Compliance and their Underlying Technologies

<table>
<thead>
<tr>
<th>Key solutions areas</th>
<th>Underlying technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Security solutions for unambiguous identity verification and bank-client interaction</td>
<td>Biometrics combined with deep learning; cryptography, distributed ledger technology</td>
</tr>
<tr>
<td>2. Automated detection of suspicious behavior on payments and client systems</td>
<td>Machine learning, artificial intelligence</td>
</tr>
<tr>
<td>3. Big data infrastructures: data ingestion, storage, visualization and analysis</td>
<td>Increased computing power, improved and cheaper data storage, faster data connections, cryptography, topology, artificial intelligence</td>
</tr>
<tr>
<td>4. Automated execution of AML/KYC investigations: analysis of internal and external data sources</td>
<td>Robotics and AI, big data infrastructures</td>
</tr>
<tr>
<td>5. Shared utilities and centralized data repositories</td>
<td>Cryptography and, in the future, possibly distributed ledger technology</td>
</tr>
</tbody>
</table>

A practical case⁶ with the application of artificial learning to improve AML detection in correspondent banking:

In the case, the global bank’s existing AML efforts relied on sorting static account information using predetermined rules. This process resulted in poor identification of suspicious activity, wasted investigator efforts, and overall low efficiency. Subsequently, by deploying advanced and objective machine learning to analyse existing transaction data and identify anomalous behaviours in its correspondent banking operations, the bank achieved reductions in investigative volume of more than 20% while lowering regulatory exposure by discovering new risk segments that had previously gone unnoticed. This resulted in the bank investigators being able to effectively focus on actual suspicious behaviour and minimise false positive investigations; the bank deployed such TMS technique in correspondent banking globally.

Therefore, it is evident that with the adoption of intelligence/technology innovations, e.g., robotics process automation, artificial intelligence/machine learning, etc., for some strategic pivotal processes when performing TM of correspondent banking, the TM processes could be augmented from a traditional rules-based model to enhance the overall TM methodological mechanism with more accurate and quality alerts generation, thus strengthening the effectiveness and efficiency of the ultimate TM program.


a. From Global Perspective, e.g., International Bodies

The latest international guidance paper on correspondent banking was released by BCBS in June 2017. By and large, application of regulatory oversight to CBRs by the issuance of global CBRs guidance papers on one hand, the high degree of self-disciplined regulatory approach was adopted by global regulators on the other hand. However, since the 9/11 issue in world history, global regulators noticed leniency could not be tolerated anymore, thus, more stringent and more details in know-your-customer information has to be obtained to be current. Due to the shift of correspondent banking business from high-margin/high-risk to low-margin/high-risk market, “de-risking”/termination of CBR business has been noticed among industry players.

b. From a Specific Jurisdiction Perspective, e.g., Hong Kong (HK)

Domestically, AML/CFT regulatory regime in HK follows international standards issued by:
- FATF Guidance on Correspondent Banking Services (October 2016)
- BCBS Sound management of risks related to money laundering and financing of terrorism (Annex 2 – Correspondent Banking, June 2017)
- Wolfsberg Publication of Guidance paper on RMA relationships Due Diligence (2016)
- Wolfsberg AML Principles for Correspondent Banking (2014)

In HK, in addition to adherence to the above international standards and guidance, local government and banking regulators also publicised a specific guidance paper and report relating to TM:
- FATF Mutual Evaluation Report of Hong Kong (September 2019)
- Hong Kong ML and TF Risk Assessment Report (issued by HK government in April 2018)
- Guidance Paper on Transaction Screening, Transaction Monitoring and Suspicious Transaction Reporting (Revised May 2018)
- HKMA AML/CFT Guideline (For Authorised Institutions) (Revised October 2018)

The FATF HK Report recognises that Hong Kong has a strong legal foundation and effective system for AML/ CFT. The HK ML and TF Risk Assessment Report, in reference to the FATF HK Report, also recognised that despite correspondent banking exposing banks to higher ML vulnerabilities (because the correspondent bank often has limited information on the parties or the purpose and nature of underlying transactions), however, correspondent banking business in Hong Kong is assessed to have lesser vulnerabilities because, compared with some other products or services such as private banking, local banks maintain limited numbers of relationships with banks from higher-risk jurisdictions, and their use payable-through accounts is comparatively low and subject to identification and close monitoring. For example, testing has shown that banks’ understanding of correspondent banking vulnerabilities and their ability to mitigate them have improved, e.g., through the quality of payment message information. This has also improved banks’ ability to manage related sanctions risks.

7. Case Studies

Case 1 – Westpac

Westpac accused of more than US$ 23M breaches of AML laws

Austrac launches legal action against bank over $11bn in transactions and allegedly failing to detect activity ‘indicative of child exploitation.’

Australia’s financial intelligence agency has launched legal action against Westpac, one of the country’s biggest banks, accusing it of more than 23m breaches of anti-money laundering and counter-terrorism finance laws involving $11bn in transactions, including transfers potentially linked to child exploitation.

In a statement filed with the federal court, Austrac said Westpac had failed to “carry out appropriate due diligence on customers sending money to the Philippines and South East Asia for known child exploitation risks.”

Austrac said Westpac had been aware of the child exploitation risks relating to low-value payments made through one of its systems, LitePay, since 2013 but had not fixed them until June 2018.

---

Red-Flags Indicators / Lessons Learned

- Failure to report international funds transfers
- Origins of international funds transfers
- Correspondent banking lapses
- Inadequate AML/CFT Programme
- Child Exploitation

Case 2 – HSBC

US Vulnerabilities to Money Laundering, Drugs and Terrorist Financing: HSBC Case History

HSBC is one of the largest FIs in the world, with over $2.5 trillion in assets, 89 million customers, 300,000 employees, and 2011 profits of nearly $22 billion.

Its key US affiliate is HSBC Bank USA NA (HBUS). HBUS operates more than 470 bank branches throughout the United States, manages assets totalling about $200 billion, and serves around 3.8 million customers. It is headquartered in McLean, Virginia, but has its principal office in New York City.

It is reported that HSBC acquired its US affiliate, not just to compete with other US banks for US clients, but primarily to provide a US platform to its non-US clients and to use its US platform as a selling point to attract still more non-US clients. HBUS’ correspondent services, thus, provide policymakers with a window into the vast array of money laundering and terrorist financing risks confronting the US affiliates of global banks.

The Subcommittee, (the Permanent Subcommittee on Investigation of US), examined HSBC because of its weak AML program. In September 2010, as a result of its investigation, the Subcommittee has focused on five issues illustrating key AML and terrorist financing problems that continue to impact correspondent banking in the United States. They include opening US correspondent accounts for high risk affiliates without conducting due diligence; facilitating transactions that hinder US efforts to stop terrorists, drug traffickers, rogue jurisdictions, and other from using the US financial system; providing US correspondent services to banks with links to terrorism; clearing bulk US dollar travelers cheques despite signs of suspicious activity; and offering high risk bearer share corporate accounts. Avoiding the money laundering risks involved in these activities requires an effective AML program, with written standards, knowledgeable and adequate staff, the infrastructure needed to monitor account and wire transfer activity for suspicious transactions, effective AML training, and a compliance culture that values obtaining accurate client information. In addition to focusing on these five issues at HBUS, the Subcommittee investigation examined the regulatory failures that allowed these and other AML problems to fester for years.

Red-Flags Indicators / Lessons Learned

- Servicing high-risk affiliate
- Circumventing OFAC prohibitions
- Disregarding links to terrorism
- Clearing suspicious bulk Travelers Cheques
- Offering suspicious corporate accounts
- Regulatory failures

---


8. Conclusion

In conclusion, as analysed in sections 3 and 4 above, one must not apply one-size-fit-all approach when conducting transactions analysis and investigation during TM for different types of businesses banking, namely private banking, corporate banking and correspondent banking. It is recommended that different businesses banking, especially correspondent banking, can apply the TMS methodology/framework in order to adjust their TMS tailor to their specific bank situation.

By adopting the procedural cycle, the essential components of TM methodology and each process’s specific techniques, an effective TMS and management program for correspondent bank relationships could be properly applied via:

Effective TM Program, Management Cycle, and Methodology

1. FI counterparty segmentation
2. Anomaly activities/behaviours profiling
3. Scenarios setting
4. Tuning optimal thresholds values/parameters to scenarios setting
5. Ongoing tuning of optimal thresholds values and suspicious TM scenarios
6. Ongoing TM of correspondent bank relationships
7. Ongoing TM of non-customer correspondent bank relationships

Illustrative example⁵₀:

In addition, an augmented TM process could be achieved via intelligence application at some strategic pivotal process of the TM cycle to enhance the overall TM methodological mechanism with more accurate and quality alerts generation, thus strengthening the effectiveness and efficiency of the ultimate TM program.

An Augmented TM Program⁵¹

---

⁵₀ Reference source: Symphony Ayasdi, A Longer Lever for AML: Intelligent Alerts, Typologies and Segmentation, 24 Oct 2017
⁵¹ Reference source: Symphony Ayasdi, White paper: AML Solution Deep Dive, 2019
9. References


Hong Kong Institute of Bankers. (2013, May). *Banking industry commercial / corporate banking specification of competency standards*.


Hong Kong Monetary Authority. (2018, October). *Guideline: AML/CFT (for authorized institutions)*, s.5.6, s.5.7.


Piwowarska, A. (2019, 8 February). *AML transaction monitoring overview: Banking segments differentiators - Retail, corporate, correspondent and investment banking*.


Qatar Financial Centre Regulatory Authority. (2018, May). *Guidance on correspondent banking services*, Figure 1.


SWIFT Message Type Reference (November 2019). *Example 1: MT 205 COV as cover of MT 103*, Retrieved from: https://www2.swift.com/knowledgecentre/publications/us2m_20190719/2.0?topic=mt205cov-example-0.htm


Symphony Ayasdi, A Longer Lever for AML: Intelligent Alerts, Typologies and Segmentation, 24 Oct 2017


10. Appendices

Appendix 1 – SWIFT Message Graphical Illustrations

SWIFT Message MT 103 Customer Transfer with Currency Conversion

Consortia Pension Scheme, a corporate in Zürich requests its bank (BNKACHZZ) to execute a pension payment in Swiss Francs. The beneficiary has his account with the Belgian correspondent of BNKACHZZ.

Information Flow

---

<table>
<thead>
<tr>
<th>Ordering Customer</th>
<th>Consortia Pension Scheme Zürich</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>BNKACHZZ</td>
</tr>
<tr>
<td></td>
<td>MT 103</td>
</tr>
<tr>
<td>Receiver</td>
<td>BNKBBEBB</td>
</tr>
<tr>
<td>Beneficiary Customer</td>
<td>Johann Willems Brussels</td>
</tr>
</tbody>
</table>

SWIFT Message MT 202 COV as cover of MT 103

Mr. Big orders Bank A, Brussels to pay USD to Mr. Small with Bank B, London. Bank A processes this transaction through cover method by sending:

1. A customer credit transfer message MT 103 to Bank B.

Information Flow

---

52 SWIFT Message Type Reference (November 2019). Example 1.6: Customer Transfer with Currency Conversion, Retrieved from: https://www2.swift.com/knowledgecentre/publications/us1m_20190719/2.0?topic=mt103-example-0-6.htm
53 SWIFT Message Type Reference (November 2019). Example 1: MT 202 COV as cover of MT 103, Retrieved from: https://www2.swift.com/knowledgecentre/publications/us2m_20190719/2.0?topic=mt202cov-example-0.htm
SWIFT Message MT 205 COV as cover of MT 103

Mr. Big orders Bank A, Brussels to pay USD to Mr. Small with Bank B, London.

Bank A processes this transaction through cover method by sending:

1. A customer credit transfer message MT 103 to Bank B.

Information Flow

---

SWIFT Message Type Reference (November 2019). Example 1: MT 205 COV as cover of MT 103, Retrieved from: https://www2.swift.com/knowledgecentre/publications/us2m_20190719/2.0?topic=mt205cov-example-0.htm
## SWIFT Message Types

<table>
<thead>
<tr>
<th>MT</th>
<th>MT Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>103</td>
<td>Single Customer Credit Transfer</td>
<td>Instructs a fund transfer.</td>
</tr>
<tr>
<td>202</td>
<td>General Financial Institution Transfer</td>
<td>Requests the movement of funds between financial institutions except if the transfer is related to an underlying customer credit transfer that was sent with the cover method, in which case the MT 202 COV must be used.</td>
</tr>
<tr>
<td>202 COV</td>
<td>General Financial Institution Transfer</td>
<td>Requests the movement of funds between financial institutions, related to an underlying customer credit transfer that was sent with the cover method.</td>
</tr>
<tr>
<td>205</td>
<td>Financial Institution Transfer Execution</td>
<td>Further transmits a transfer request domestically except if the transfer is related to an underlying customer credit transfer that was sent with the cover method, in which case the MT 205 COV must be used.</td>
</tr>
<tr>
<td>205 COV</td>
<td>Financial Institution Transfer Execution</td>
<td>Further transmits a transfer request domestically, related to an underlying customer credit transfer that was sent with the cover method.</td>
</tr>
<tr>
<td>910</td>
<td>Confirmation of Credit</td>
<td>Advises an account owner of a credit to its account.</td>
</tr>
<tr>
<td>950</td>
<td>Statement Message</td>
<td>Provides balance and transaction details of an account to the account owner.</td>
</tr>
</tbody>
</table>

## Appendix 2 – Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACFCS</td>
<td>Association of Certified Financial Crime Specialists</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>BCBS</td>
<td>Basel Committee on Banking Supervision</td>
</tr>
<tr>
<td>BIS</td>
<td>Bank for International Settlements</td>
</tr>
<tr>
<td>CBR</td>
<td>Correspondent Banking Relationship</td>
</tr>
<tr>
<td>CB</td>
<td>Correspondent Banking</td>
</tr>
<tr>
<td>CPMI</td>
<td>Committee on Payments and Market Infrastructures</td>
</tr>
<tr>
<td>DCS</td>
<td>Direct Currency Shipment</td>
</tr>
<tr>
<td>FFIEC</td>
<td>Federal Financial Institutions Examination Council</td>
</tr>
<tr>
<td>Fi(s)</td>
<td>Financial Institution(s)</td>
</tr>
<tr>
<td>FSB</td>
<td>Financial Stability Board</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorism Financing</td>
</tr>
<tr>
<td>JMLSG</td>
<td>The Joint Money Laundering Steering Group</td>
</tr>
<tr>
<td>OFAC</td>
<td>Office of Foreign Assets Control</td>
</tr>
<tr>
<td>ML</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>PTA</td>
<td>Payable-Through Account</td>
</tr>
<tr>
<td>SWIFT</td>
<td>The Society for Worldwide Interbank Financial Telecommunication, legally S.W.I.F.T. SCRL</td>
</tr>
<tr>
<td>TM</td>
<td>Transaction Monitoring</td>
</tr>
<tr>
<td>TMS</td>
<td>Transaction Monitoring System</td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
</tbody>
</table>