idetect

Real-time AML Detection in Money Service Businesses: Benefits at a Time of De-risking and Increased Regulatory Pressure

Contents

Introduction

The second decade of this millennium has been marked with tremendous pressure on banks and other non-banking financial institutions to conform to Know Your Customer norms of understanding their customers in terms of their businesses and transactions. The use of numbered accounts, shell banks and shell companies to avoid the disclosure of the true identity of customers and beneficiaries was the primary concern of regulators. Over time, the focus shifted to methodologies used to move money from one place to another with minimal—if any—data disguising the true owners or beneficiaries of the funds.

The Governments, primarily through the Financial Action Task Force (FATF) and the European Parliament (EU AML Directives), have designed recommendations, guidance, directives and requirements to identify and correct these occurrences. They increased the number of predicate offenses covered under "Money Laundering" and "Terrorism Financing" by including criminal actions like "tax evasion," "proliferation," "window-dressing" and "money mulling" and re-assessed the penalties & fines imposed on financial services providers in the event of non-compliance. Under these strict measures, large banks with a global presence were penalised with millions or billions of dollars for assisting money laundering or terrorism financing. The regulators are making sure that the message is sent loud and clear that they will no longer tolerate non-compliance.

The banks—having been fined or being under threat of heavy fines and loss of reputation—have taken severe measures to apply new risk ratings to their customers, business partners, correspondents, etc. They applied de-risking measures (including closing accounts and stopping the process of opening new accounts) to their customers and non-banking financial service providers who were not equipped to adequately implement anti-money laundering and anti-terrorism financing measures. In this way, banks prevented being involved directly or indirectly due to the high risk of regulatory violations.

One sector of business that was directly affected by this de-risking from banks was the non-banking financial sector. This includes money transfer and remittance companies (the so called "Money Service Businesses" or MSBs), which are used mostly for specialised products such as low-cost money remittances/transfers for un-banked private individuals. Even though the MSBs receive a lot of cash for their products or services, they cannot have access to bank accounts due to de-risking. The flow of funds then, from the individual sender up to the ultimate beneficiary, cannot be transferred easily and through standard banking correspondent channels. Consequently, they may create or use different channels that increase the risk of money laundering and terrorism financing. This is a vicious circle and an endless story, as many MSBs were forced to close down or forced to invest in technology to control the data and flow of funds within the regulatory requirements.

A real-time detection system is one that enables the financial services provider to identify, investigate and manage money laundering and terrorist financing risks before even engaging into a transactional contract. The real-time detection system identifies risk areas based on rules and scenarios, identifies persons that are either listed for sanctions or bad-publicity and assists the

compliance investigators to apply a risk-based approach in their decision to accept or reject the transactional contract. Banks are investing in such technology and expect the MSBs or other non-banking financial services providers to do so too; it is part of their continuous compliance assessment and they do apply de-risking to those MSBs that do not adhere to the requirements for real-time detection of money laundering and terrorism financing risks.

Real-time detection systems are software solutions designed to process related data and analyse, identify & alert financial crime investigators for any possible financial crime risk — this is not limited to just money laundering or terrorism financing. Even though money laundering and terrorism financing are prime risks for the Compliance Officers, other financial crimes like violations of sanctions, financial fraud, financial security breaches and bribery (among others) can be detected if the system is appropriately configured. Such real-time detection systems use a variety of technologies to accomplish this, such as matching algorithms, mathematical statistics, profiling methodologies, validation rules, analytical scenarios and machine learning. These are performed on a real-time basis to identify personal attributes/profiles and transactional behavioural patterns in order to alert financial crime investigators about various risks related to customers and their transactions. Detection systems are capable of stopping the funds process flow immediately in order to allow time for the financial crime investigator to assess and analyse identified risks and, via a real-time response workflow, decide if the transaction is accepted or rejected based on the financial service provider's risk appetite.

The idetect® software is a pioneer of real-time anti-money laundering (AML) detection and is fully compatible with Compliance Officer requirements based on official regulations and internal financial crime risk management policies and procedures. idetect® offers a holistic user interface to the financial crime investigator and Compliance Officer, enabling them to independently make compliance decisions using analytical data and meaningful information provided by the system within milliseconds. Through its modern and advanced technology, idetect® uses machine-learning technologies to reduce false positives and increase the efficiency of adequate financial crime investigations.

Banks, large money transfer & remittance companies, and other types of MSBs invest in the idetect® software to implement adequate compliance controls required by their Correspondent Banks and thus avoid any de-risking measures taken against them. In addition, they fully satisfy regulatory requirements on anti-money laundering and counter financing of terrorism for adequate compliance measures and controls.

idetect® is currently the only solution on the market capable of offering performant and efficient fully real-time AML profiling and monitoring.

Banks, MSBs and the Regulatory Environment

Banks are financial services providers that are licensed and regulated in order to provide a wide range of financial products and services to their customers. Their customer portfolio can include individuals, corporates, governments and government-owned organisations, other financial service providers, other banks, etc. Through the years, regulators imposed requirements and controls on the Banks that limited their business scope or forced them to apply adequate risk management for every type of business vertical that they engaged in. Many of them were penalised heavily or forced to close-down their operations because they were unable to apply adequate measures to control funds that were entering into the worldwide financial system from illegal or doubtful sources. In this way, the cost of compliance due to the increased pressure from regulatory requirements affected their profitability and they were forced to take de-risking measures.

A money transfer and remittance company—a Money Service Business (MSB)—is a company that can be fully licensed and regulated in a country or provide a technological platform to other MSBs to process remittance transactions and funds transfers worldwide without a license. The difference between the two is the need for regulatory compliance.

The money remittance company, or Exchange House, is fully licensed by the regulator in the country or region it operates. There is no differentiation in regulatory compliance requirements if they offer their remittance products through physical branch locations or through technological distribution channels. They must comply with both the laws of the country and regulatory requirements, especially those related to money laundering and terrorism financing.

The money transfer company, however, is not licensed to offer remittance products directly to customers. They are therefore not regulated by any formal regulator in one or more countries, but they use agents that execute remittance transactions through their technological platform. The agents can be licensed and regulated or not, according to the location, country or region.

Over the last decade, many FinTech companies were created to provide technology and platforms that bridge or link together money remitters in order to execute transactions easily, faster and at a lower cost. Moreover, the data capturing formalities, as described by a country's laws and regulations, are not strictly followed. Blockchains, clearing agents, money remitter technologies, cards, e-wallets and other FinTech products add to the overall business risk and possibly reduce control measures used by FinTech-associated MSBs. This creates an additional compliance issue for otherwise licensed and regulated money remittance companies.

Banks are prohibited by regulators to engage in any kind of business that cannot be subject to end-to-end controls. Many of them are not even allowed to open accounts or use their financial system integration to process remittances from non-licensed and non-regulated money remittance companies.

Balancing the Regulatory Requirements with Bank Risk Management Requirements

Regulators frequently receive and inspect independent audit reports from banks on measures taken to mitigate money laundering and terrorist financing risks. These inspections concentrate on high-risk business areas, including account transfers, customer money remittances, end-to-end correspondent controls, etc. Banks are therefore applying equal requests to MSBs in such a way that they are forced to implement end-to-end compliance controls.

Common measures applied by banks include:

- Design and implement an adequate AML/CFT Compliance and Sanctions Programme;
- Employ a professional Compliance Officer to implement the AML/CFT Compliance and Sanctions Programme;
- Continuously train all employees on AML/CFT Policy and Procedures;
- Periodically review the implementation of the AML/CFT Policy and Procedures in terms of effectiveness;
- Deploy adequate AML software to meet the advanced requirements of end-to-end controls for all executed transactions; and,
- Employ an independent AML reviewer to audit the design and implementation of adequate systems and controls within the MSB.

On an annual basis, banks should request to receive an independent AML review executed by the MSB. If further points need to be clarified, they may either request further independent review or even direct a review by the Bank Compliance Team.

The MSBs are forced to maintain a good balance between regulatory and bank requirements — they also need to keep a balance in the way they operate their business. The pressure on the MSBs is to maintain a high standard of compliance control, yet this also increases operating cost and the discomfort within the management teams. It is a tough decision that has to be taken: Compliance vs Business.

Increased Pressure from Regulators to Banks

The regulators are implementing FATF Recommendations[1] and FATF Guidance[2] (which are internationally endorsed standards against money laundering and terrorist financing), adapting their legal and regulatory frameworks to increase transparency and implementing actions against the illicit use of the financial system. In this respect, regulators require banks and MSBs to adapt immediately to the new framework and take appropriate measures to independently review the adequacy of these measures.

According to the Boston Consulting Group,[3] "The number of individual regulatory changes that banks must track on a global scale has more than tripled since 2011, to an average of 200 revisions per day." How can banks adapt to, and track, all of these changes? They need a dedicated compliance team and systems & procedures to keep control of the business based on new and changing requirements. A catalyst to action is the constant risk of uncontrolled fund transfers and an unawareness of the money flow through accounts, both of which result in hefty fines.

Reuters[4] published an article relating to fines that banks around the world were forced to pay; the article states that "Banks across the world have paid about USD321 billion in fines since the 2007-2008 financial crisis as regulators stepped up scrutiny, according to a note by the Boston Consulting Group." It is not something that the U.S. Government has pioneered but, according to the same article, "their counterparts in Europe and Asia are likely to step up pace."

The top four cases of recent international bank fines include[5]:

1. **Wachovia** (U.S. - currently part of Wells Fargo): Found to be involved in money laundering related to Mexican drug cartels. The money received from drug deals was delivered to money exchangers in Mexico, who then deposited these funds into Mexican bank accounts. The Mexican banks did not validate the origin of the funds and, ultimately, the money passed from them to Wachovia. Though Wachovia returned the funds back to the originating country, they still had to pay U.S. federal authorities a total of GBP123.7 million for willingly failing to establish an adequate AML program;

2. **Standard Chartered Bank** (UK): Accused of helping the Iranian government to circumvent U.S. money laundering regulations for 10 years. The bank paid GBP262 million to the U.S. (2012) for failures in anti-money laundering controls and for violation of sanctions related to Iran, Burma, Libya and Sudan. In 2014, it had to pay an additional GBP232 million to the U.S. for failure to control and flag suspicious transactions; it was also forced to discontinue maintaining certain high-risk

[1] http://www.fatf-gafi.org/publications/fatfrecommendations
[2] http://www.fatf-gafi.org/documents/guidance
[3] Global Risk 2017 – Staying the Course in Banking; March 2017, Boston Consulting Group
[4] https://www.reuters.com/article/banks-fines/banks-paid-321-bln-in-fines-since-financial-crisis-bcg-idUSL2N1GF20L
[5] https://www.int-comp.com/ict-views/posts/2016/07/22/top-5-money-laundering-cases-of-the-last-30-years/

customers at its United Arab Emirates branch;

3. **BCCI** (UK): Accused of direct involvement in money laundering, corruption and fraud. The bank was forced to pay GBP11.3 million for money laundering. Later, the Bank of England had to close down the operations of the bank following an independent investigation, resulting in a loss of GBP10 billion of creditor money still owed to-date.

4. **HSBC** (UK): Had to pay GBP1.2 billion to the U.S. in 2012 for having inadequate controls. The bank was accused of supplying banking services and U.S. dollars to Saudi Arabian banks connected to terrorist financing, dodged restrictions created to prevent transactions involving Iran, North Korea, and other countries subject to sanctions, and failed to properly categorise Mexican customers as "high-risk" even if they were involved in drug trafficking and money laundering.

Increased Pressure from Regulators to MSBs

The regulators are also considering the risk for every member within their financial system. They assess and categorise the financial service providers according to the exposure they have to money laundering and terrorism financing.

As part of the FATF Mutual Evaluation[6] executed in every country, FATF is publishing a report of findings that are highlighting the level of implementation of adequate anti-money laundering and counter terrorist financing measures within its financial system. In such a report, FATF is considering the overall legal framework of the country in relation to money laundering and terrorism financing, the controls implemented in order to mitigate AML/CFT risks and the effectiveness of their internal evaluation and assessments. Based on this mutual evaluation report, FATF can downgrade the country and publish its deficiencies to all its members. The latter has an effect on many financial aspects of the country, including the de-risking imposed on the banks and MSBs operating in the country.

Based on unofficial information from different regulators and on the stricter controls applied, MSBs are considered to pose a significant risk in relation to other financial service providers. As an example of the risk between a MSB and the potential of affecting its home country's financial system, the United States of America—even though it has a highly regulated financial system—does not allow the operation of MSBs unless they can control & approve the opening of new accounts in U.S. Dollars in U.S. banks.

United Arab Emirates is a unique example where MSBs have a significant presence. A great number of MSBs operate within the country and, comparative to the size and population of the country, they are an extremely important growth market. However, though the growth of the MSB sector has been phenomenal over the last few years, UAE regulators are now implementing strict controls over the level of compliance in relation to anti-money laundering and counter terrorist financing laws and regulations. Furthermore, UAE regulators have downgraded the license of MSBs: on 11th June 2018, the Central Bank of the UAE issued a public statement[7] whereby remittance activities are limited to seven (7) exchange houses. In addition, public warnings have been published in the local press advising the public to avoid using these exchanges for any type of remittance.

In September 2017, the Kingdom of Saudi Arabia followed suit by implementing de-risking measures on exchange houses[8] due to non-adequate controls related to money laundering and terrorist financing. Another notable development in Saudi Arabia is the fact that only 4 MSBs have a license to operate and execute cash remittances inside and outside the Kingdom.[9]

[6] http://www.fatf-gafi.org/publications/mutualevaluations/

[7] https://www.centralbank.ae/en/pdf/pressrel/PressRealse11062018.pdf

[8] https://gulfnews.com/business/sectors/banking/saudi-central-bank-suspends-money-transfers-at-three-currency-exchange-houses-1.2095579

[9] http://www.sama.gov.sa/en-US/BankingControl/Licensed%20Entities/MONEY%20EXCHANGERS_EN.pdf

The De-risking that Banks Apply to MSBs

Regulatory pressure for full compliance to laws and regulations related to Anti-Money Laundering and Counter Financing of Terrorism (coupled with the already-paid or expected implementation of fines and penalties to banks for non-compliance), almost all banks in the world are now being forced to take de-risking measures, partly or fully, on MSBs.

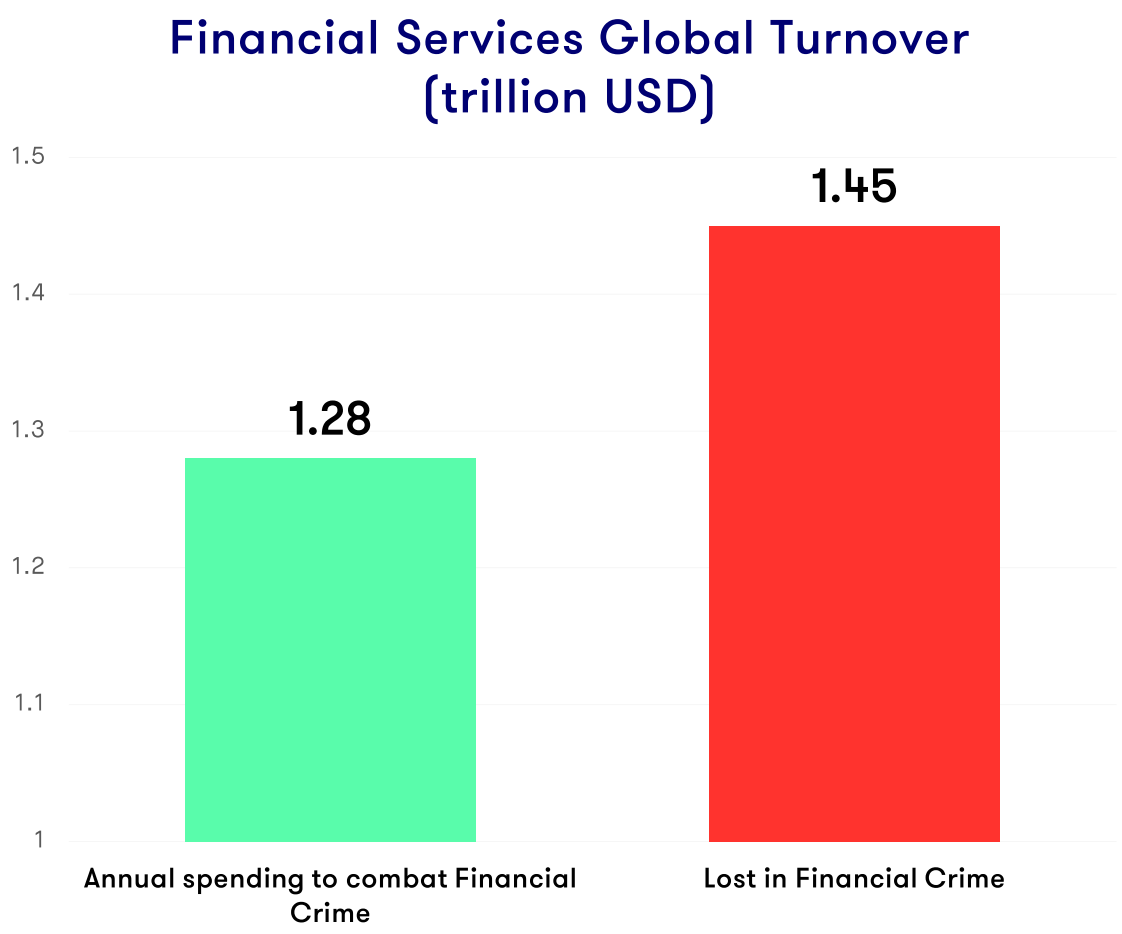
Examples of these de-risking measures include the non-opening of new U.S. Dollar denominated accounts for MSBs in the U.S. and the closing of a majority of existing accounts. There is now a heavy reluctance to open any type of account at MSBs in Europe, Middle East, Asia-Pacific and Australia. Other measures include the non-acceptance of bulk cash deposits from those MSBs that maintain an account, non-acceptance of "nested relationships"[10] or third-party transactions and the scrutinisation of every transaction on a real-time basis.

Another matter of great concern to banks is the increasing cost of compliance vs. benefit from accounts maintained for MSBs. All of this falls under the umbrella of "Financial crime," which is a broad term used to include crimes related to money laundering, terrorism financing, proliferation, fraud, corruption, bribery, human trafficking, illegal trade, drug trafficking, cyber-crime and hacking. To understand all these risks within their business verticals, banks have heavily invested—and continue to invest—in people and technology.

Per Thomson Reuter's Special Report, "Revealing the True Cost of Financial Crime,"[11] the aggregated loss of turnover due to financial crime has been estimated to be USD1.45 trillion among the organisations researched. This represents 3.5% of their annual turnover; moreover, the same organisations spent USD1.28 trillion, (representing 3.1% of their annual turnover) to combat financial crime.

[10] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf, page 11 – footnote 21

[11] "Revealing the True Cost of Financial Crime 2018 Survey Report", page 5; Thomson Reuters – www.risk.tr.com



Source: "Revealing the true cost of financial crime", 2018 survey – Thomson Reuters; www.risk.tr.com

Among the most important findings is the fact that there is a continuous screening shortfall; around 41% of their global customers, third party vendors, suppliers and/or partners were never screened. This increases the banks' risk and also magnifies pressure from regulators to implement—and request implementation for—adequate controls.

Historically, How the Practice is Applied

Money laundering existed for thousands of years, starting from the merchants of ancient history trying to hide money and avoid paying taxes to the rulers. At the beginning of the twentieth century, the U.S. imposed restrictions on money coming from illegal and gangster activity, which led to banks reporting the transactions to the authorities above a certain threshold/limit. These reporting requirements were more intensive during the 1980s when the U.S. government initiated the strict control of transactions related to drug dealing and other crimes; during this time the government also introduced the Suspicious Activity Reporting (SARs) requirement, which is still followed today. In order to understand suspicious transactions, banks collected statistics about the customers and their transactions which led to "profiling" checking; they used technology and issued customer statements which convey transactional behaviour for specific periods.

After the September 11th, 2001 terrorist attack in the U.S. and the implementation of the U.S. Patriot Act, banks and MSBs went to great lengths to avoid any kind of involvement in the use of the financial system for both terrorism financing and money laundering. Banks and other non-banking financial service providers, including MSBs, used to have simple screening solutions — mostly manual searches in public or private databases for name matches within remittance messages. In this way, they tried to find any individuals or corporate entities involved in money laundering or terrorism. Through the years, and based on the increased development of pressure from legal and regulatory requirements for further controls of all financial crime risks, banks and MSBs started investing in policies, procedures and systems to comply.

IT companies introduced specialised products for sanction screening and transaction monitoring since 2003-2004, such as solutions for SWIFT payments and for other types of money transfers. However, what was important was the implementation cost vs the regulators requirements. For this reason, although banks were investing, MSBs started implementing such systems only in the last few years.

The creation by the G7 of the Financial Action Task Force (on Money Laundering) in 1989 introduced a new objective in the fight for money laundering; it was created with the tasks of monitoring the progress of its members in implementing anti-money laundering measures, reviewing and reporting on laundering trends, measures, countermeasures and promoting the adoption and implementation of anti-money laundering standards globally. The FATF Forty Recommendations were introduced in 1990 and were revised in 1996 and 2003, whereas in October 2001 the Nine Special Recommendations (initially eight and then one more added) on Terrorist Financing supplemented the anti-money laundering standards applicable to all its member jurisdictions. In February 2012, the Forty Recommendations were fully revised and are still applicable.

In these FATF Recommendations, there are a number of Articles, like Article 10 – Customer Due Diligence, Article 13 – Correspondent Banking, Article 14 – Money or Value Transfer Services and Article 16 – Wire Transfers that require sophisticated AML Systems in order to apply

appropriate controls for prevention of money laundering and terrorism financing.

Money transfer and remittance companies must therefore apply strict anti-money laundering and counter terrorism financing measures as well as other financial crime investigation controls, as these are strict regulatory requirements, corresponding bank requirements as well as market standards requirements. Non-compliance renders the company vulnerable to severe financial penalties, loss of licensing and or personal responsibility imposed on its Management and Owners.

Real-time vs. Near-time or Batch Monitoring

It is impossible for compliance to gather so much data, analyse it into meaningful information and then implement investigation techniques without appropriate tools. Technology has always played a major role in many business sectors and is also a must for investigations and transactions monitoring. Furthermore, regulators and correspondent banks want to get an assurance that MSBs apply technology in the proper way so as to support them with licensing and account maintenance, respectively.

In order for a MSB to understand what methodology to select and how to apply controls for its money transfer and remittance services, it has to fully comprehend its business model, the type and level of customer due diligence that must be executed, the data captured & maintained for every customer and transaction, transaction processing workflows and turn-around-timing. MSBs that have high automation capabilities must invest primarily in real-time AML systems, whereas others that lack either data quality or know-how to manage real-time investigations can proceed with near-time or batch processing methodologies.

A real-time anti-money laundering control processing methodology is one that gathers the data from the core transactional system just after the verification of the user to complete the remittance transaction. There are two possible workflows, either before or after the transaction receipt processing. In a near real-time processing methodology, the transaction processing and workflow is independent and outside of the applied anti-money laundering controls, but is done simultaneously in time. The batch processing is not executed near the time that the transactions processing workflow is executed (i.e., batch processing is executed after the business day closure).

There are regulators that would like to have real-time anti-money laundering measures—including sanctions and black list screening—to present to the front-line staff or the sender (if using a WebApp or Mobile App) before the completion/acceptance of the transaction and the printing of a transaction receipt — **this is real-time processing**. There are other regulators, though, that would like the transaction to be processed and sent to its destination and then apply controls such as profiling and transaction monitoring – **this is batch processing**. Other Regulators are fine with something in between – **this is near real-time processing.**

The Pros and Cons of Each Methodology

Fundamentally, the advantages and disadvantages of each anti-money laundering control processing methodology are defined by the business type of the MSB, the regulatory requirements and, most importantly, the anti-money laundering risk appetite. The MSBs have no given "loyalty" from their customers; the MSB customers can use their money transfer or remittance services once or as many times as they believe that serve their interests. Unlike banks, MSBs are "transaction-based" and not "account-based" financial service providers. In this respect, the need for immediate controls (e.g., real-time anti-money laundering processing) is more important in transaction-based financial service providers than other businesses. Banks, being account-based financial service providers, have the luxury of time to execute near-time or batch anti-money laundering processing methodologies.

Nonetheless, real-time processing is an anti-money laundering control methodology that is useful to banks and other financial service providers and should not be limited to only MSBs — it is applicable to every kind of business model. Real-time processing provides a comfort level of control to the Compliance Officer and, above all, offers an investigator the option to reject any extremely high-risk transaction on-the-spot.

For example, when transfers are sent through SWIFT® (based on FATF recommendation 16[12]), wire transfer messages must include accurate details of both the originator and the beneficiary throughout the message workflow. In the absence of real-time anti-money laundering controls, it is very difficult to comply with this recommendation without risking the freezing of funds or, in a worse case scenario, compromising the whole relationship with the correspondent. Apart from that, other risks like sanctions violations, structuring of transactions, money mulling, etc. can be identified and stopped on-the-spot by using a real-time anti-money laundering processing methodology.

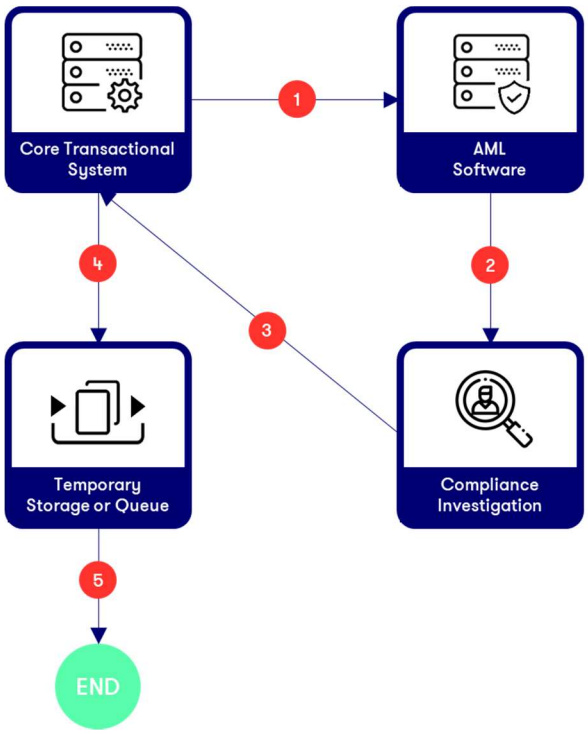
Near real-time or batch anti-money laundering processing methodologies are useful when a high volume of transactions pass through a financial service provider that lacks an advanced technical infrastructure—such as fast processing servers and networks—or the Compliance Program is divided into separate functions. The processing time may be longer, as well as being uninterrupted from further transactions processed during/simultaneously with the anti-money laundering controls. These processing methodologies can be good for identified risks for transactional profiling that have a longer periodicity (e.g., for a period of a month or quarter), whereas real-time processing methodology is more suitable for smaller periods (e.g., daily or weekly).

[12] FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, updated October 2016, FATF, Paris, France – www.fatf-gafi.org/recommendations.html

What is a Real-time AML Monitoring Methodology?

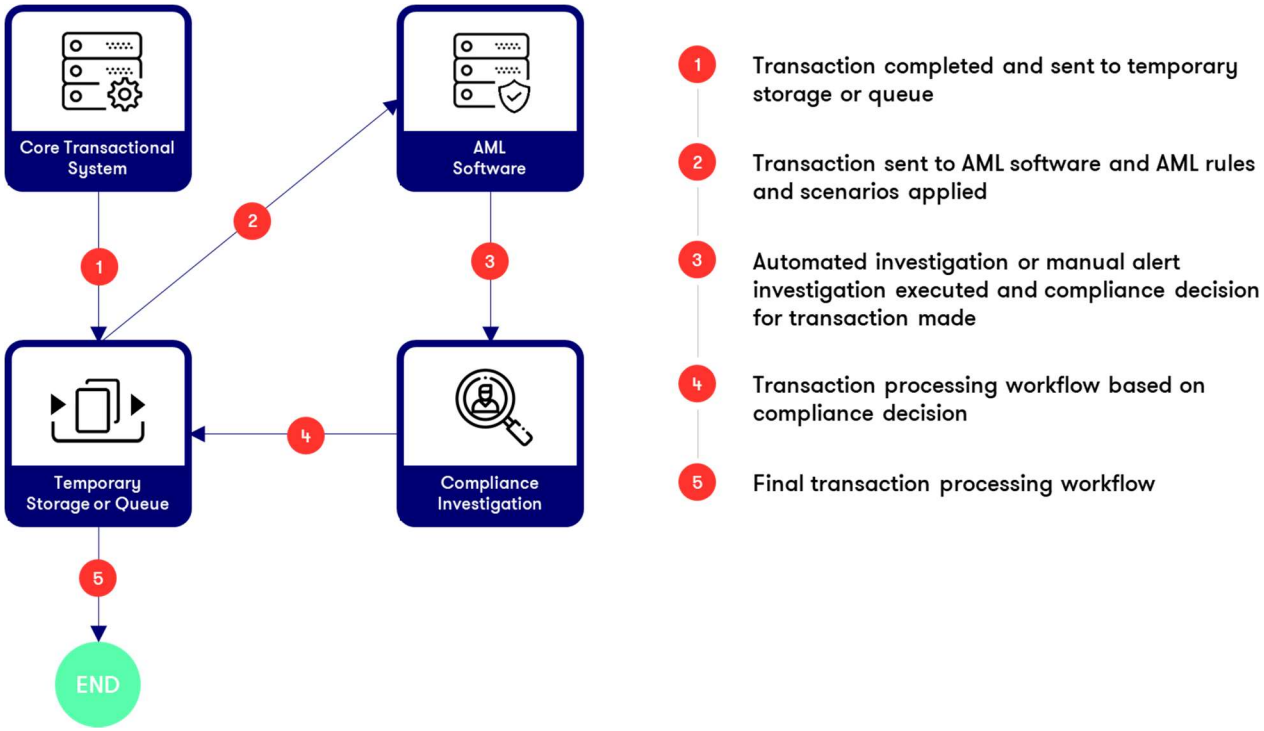
A real-time anti-money laundering monitoring methodology consists of an automated integrated solution between the core transactional system and the anti-money laundering software. The processing workflow is designed in such a way that any transaction is validated against the specified anti-money laundering rules or scenarios (other variables can be added depending on the risk appetite of the Company) before it proceeds to its final destination. There are many types of workflows that can be applied to meet the specific needs of the company and/or its business model. Two suggestions are presented below:

Type A: A transaction is frozen in the front-end until a compliance decision is made:



1. Transaction completed and sent to AML software
2. AML rules and scenario applied
3. Automated investigation or manual alert investigation executed and compliance decision for transaction made
4. Transaction processing workflow based on compliance decision
5. Final transaction processing workflow

Type B: A transaction is completed at the front-end, but temporarily frozen until a compliance decision is made:



The differences between the different workflows are related to the business model, the delivery channel and type of product. The higher the risk, the more immediate are the real-time anti-money laundering processing methodologies applied by the company.

Some of the major pros & cons of the two different types of real-time detection workflows mentioned above are:

Type A		Type B	
pros	cons	pros	cons
Some regulators require rejection of the transaction before completion at the front-end if it is related to any money laundering or terrorist financing	Some regulators require completion of any kind of transaction from the front-line user before being dealt with by compliance investigators	Some regulators require completion of any kind of transaction from the front-line user before being dealt with by the compliance investigators	Some regulators require rejection of the transaction before completion at the front-end if it is related to any money laundering or terrorist financing
There is an immediate response to the front-line user regarding completion of the transaction	There is a risk of tipping-off due to lack of due care by the front-line user	There is no risk of tipping off due to the fact that the controls are not transparent to the front-line user	The reversal of the transaction, in the case of non-acceptance, is complicated
There are AML systems that can use machine learning capabilities and speed up the automated compliance decision-making process	The cost of compliance increases due to the use of multiple compliance investigators to decide on every transaction stopped by the AML software immediately	The cost of compliance decreases due to the use of centralised compliance investigators to decide on the exceptions	There is an increase in the time taken for compliance to decide on risky transactions
Most suitable for transaction-based processes (e.g., remittances)	Not suitable for conservative business models	More suitable for conservative business models	Not preferred for continuous account monitoring (e.g., profiling)

idetect's Offering for Real-time Detection in Money Transfer and Remittance Companies

Based on expert opinions, the real-time detection anti-money laundering processing methodology represents the future for Compliance Officers. The increased pressure of regulators for tighter controls, the de-risking measures from correspondent banks and the customers' need to provide secure and fast remittance services is inevitably driving banks and MSBs towards real-time detection. This is increasingly becoming necessary to cover their anti-money laundering and counter financing of terrorism controls from end-to-end.

The design of the appropriate model for implementing real-time detection is based primarily on the company's industry, the strict regulatory environment and the business strategy. Different solution providers exist in the market, but very few can demonstrate implementations that are working and providing positive results of appropriate AML/CFT risk management.

idetect® is a market leader in implementations with prime money transfer and remittance companies throughout the world. The company provides financial crime investigation solutions that feature a proven real-time detection methodology with the following high-level functionalities:

1. **Real-time connectivity** through widely-accepted standards, like webservices, APIs, queuing technologies, etc.;
2. **Real-time response to core transactional system**: Capable of adapting to any type of transaction processing methodology (e.g., type A or type B examples provided above);
3. **Real-time processing of transactions** through well-defined compliance rules and scenarios to give acceptance or blocking results immediately;
4. **Real-time sanctions and black-list screening** of every transaction with configurable lists selected by the Compliance Officer and covering public or paid list providers, own lists or even data (structured or unstructured) downloaded from public domains or websites configured as per the business requirements;
5. **Real-time processing rules** are configurable to meet the compliance and regulatory requirements of the company and any special or company-specific detection requirements;
6. **Real-time result transmitted** to reflect the compliance decision after implementation of automated or manual investigation procedures;
7. **Real-time risk rating** of both the customer and the transaction, according to the specifically configured risk scoring model applied for the company;
8. **Real-time alert and case management** used by the compliance investigator (or other functions within the Compliance Department) so as to apply 2-eye, 4-eyes or 6-eyes principles according to the needs of the company;

9. **New generation investigative Link Analysis** that provides Compliance Officers with an in-depth, fully visual analysis of risks and hidden relations between customers, non-customers and transactions to support fast decision-making; and,

10. **Machine Learning** and **Decision Tree** for further automation and reduction of false positives, effectively enabling Compliance officers to focus on, and thoroughly investigate, real risks.

The idetect® software is developed to apply unique matching algorithms and multi-variable data validations in its matching functionalities. Its machine-learning capabilities reduce the rates of false positives and increase the efficiency of real-time detection as required by FATF Recommendation 16[13] relating to money transfers and remittances. Time is a critical factor in real-time detection methodologies — idetect® significantly increases the efficiency of anti-money laundering and counter terrorist financial controls using technology that collects valuable statistics, builds comprehensive profiles and detects red flags from transaction monitoring in real-time.

In terms of Compliance Investigation Procedures, idetect® is both intuitive, engaging and user-friendly. The solution provides a visual representation of database-sourced content from either the core transactional system or from external sources (e.g., the idetect® WebCrawler, manual input from compliance investigators). This visual investigation matrix enables compliance investigators to understand the underlying transactional workflows while supporting risk assessments executed before transaction releasing/blocking decisions are taken.

The investigation matrix and all other related content, such as comments, attached documents and notes, can be saved for future reference to present a full audit trail for the compliance investigation procedure. This is often required by regulators and correspondents in the event of a dispute.

The idetect® solution offers a fully automated list management feature with full configuration options. This enables Compliance Officers to specify a wide variety of data sources, such as public sources, private, own lists or an Internet-accessible publication. All specifications can be updated, as needed, by the Compliance Officer in order to meet the demand for real-time risk detection.

[13] FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, updated October 2016, FATF, Paris, France – www.fatf-gafi.org/recommendations.html

About Machine Learning

The rapid pace of technological development, a rising level of cybercrime and an ever-changing regulatory landscape all combine to make technology-driven compliance functionality a necessity as opposed to a mere competitive advantage.

For instance, before idetect® it was difficult—if not impossible—to distinguish a collusive clique. The format of money laundering collusions varies and such transactions are typically buried in a quagmire of normal activities. To combat this, idetect® uses vertices to convey MSB customers and uses directional connections among vertices to represent transactions between customers and their counterparts.

The deducted fundamental structure of the closed-cycle structure within a graph simplifies the detection from the complexity of the networks. Given this, one can apply supervised machine learning on top of rule-based detection — with knowledge of previous patterns, the ability to discover collusive cliques increases.

Once data is converted into a graph-based structure, unsupervised machine learning has the ability to detect hidden patterns in large data sets without prior knowledge of what a fraudulent transaction or account looks like. In addition, false positives can be discarded by identifying reasons for certain activity (investigation that normally needs to be done by an analyst) or see connections and patterns that are too complex to be picked up by straightforward rule-based monitoring.

Solution Proposal

The increasing pressure from regulations and the threat of heavy fines & penalties related to anti-money laundering and counter terrorism financing are forcing money transfer and remittance companies to re-consider their existing controls. In addition, increased regulatory requirements have forced banks with correspondent relationships with money transfer and remittance companies to implement de-risking measures, such as account closures and/or closely controlling all executed transactions. New accounts are extremely difficult to open as the cost of compliance for these types of accounts have increased dramatically for correspondent banks all over the world.

What will money transfer and remittance companies do to overcome the restrictions so that they can continue to open and maintain accounts? The solution is to implement adequate and proven **real-time detection anti-money laundering methodologies and systems** that will empower them to identify, investigate and adequately manage all possible transactional risks. There is a need to invest in technological solutions that provide control functionality over end-to-end transaction workflows on a real-time basis, leaving no space for ambiguities or lapses in anti-money laundering risk management measures. The latter will be assessed by the regulators and correspondent banks and will provide them the appropriate level of comfort to allow the money transfer and remittance company to continue to operate.

The idetect® software has all the necessary technology to support a full real-time detection anti-money laundering methodology that facilitates end-to-end controls in money transfer and remittance companies. The solution is proven to be unique on the market and, where it has been implemented, regulators and correspondent banks can be assured that adequate real-time controls are in place, effectively reducing relevant risk ratings.

idetect: Key Differentiating Factors and Strengths

idetect®	Other Solutions
All features are integrated in a single tool (no need to use multiple modules).	Disparate tools with incomplete functional coverage (e.g., AML and KYC are 2 different products/modules).
Advantage Fully comprehensive platform, no need to reinvest or buy separate tools: ROI is high.	Advantage No advantage for the clients. Software vendors can charge clients higher costs.
Disadvantage None.	Disadvantage Incomplete platform, need to reinvest or buy separate tools: ROI is low. Holistic surveillance becomes impossible. Higher maintenance and upgrade cost.
All behaviour profiling can be executed in real-time either through RESTful webservice or Message-Oriented Middleware, including SWIFT connectivity.	Behaviour profiling is only done in batch.
Advantage Suspicious patterns are detected and can be stopped immediately when they occur. Batch screening is still possible for those who cannot integrate in real-time.	Advantage None.

Disadvantage None.	Disadvantage Outdated integration and technology; suspicious patterns are detected the next day, at best.
Usage of multiple recent matching algorithms, Decision Tree and Machine Learning for name-screening. Handle non-Latin characters including transliteration.	Usage of Fuzzy matching logic: regular phonetic algorithm (e.g., Soundex, Methaphone), similarity metric algorithm (e.g., Levensthein) for name-screening. Levenshtein is 1965, Soundex is 1918 and Metaphone is 1990. Impossible to screen non-Latin characters in Fuzzy logic.
Advantage Lowest possible level of false positives and false negatives. Less human intervention is needed and less errors: ROI is high.	Advantage None.
Disadvantage None.	Disadvantage High level of false positives and false negatives. Limitations for non-Latin characters. Manual intervention results in human errors: ROI is low.
Fully integrated KYC / SWIFT Screening / Ongoing Due diligence which can be executed in real-time either through RESTful webservice or Message-Oriented Middleware, including SWIFT connectivity.	Disparate KYC/SWIFT/Ongoing Due Diligence processing.

Advantage All identity and name checks are detected and can be stopped immediately when they occur. Links can be established between the channels: ROI is high.	**Advantage** None.
Disadvantage None.	**Disadvantage** If for instance SWIFT screening is handled by one tool whilst KYC is handled by another, then it is not possible to have a holistic view of the risks within your organisation. Silos are created throughout the enterprise. ROI is low.

New Gen Dynamic Link Analysis and Map interactions are fully embedded in tool.	Static display of relationship and map visualisations or no visualisations at all.
Advantage Ideal graphical display for understanding data and interacting with it online. Investigators do their work more efficiently: ROI is high.	**Advantage** None.
Disadvantage None.	**Disadvantage** Visualisations are static (e.g., diagram used to display flows instead of having a fully dynamic interaction) or do not exist, significantly limiting the capabilities of the investigators.

Use Web Crawlers to gather unstructured information from publicly available sources on the World Wide Web to produce additional actionable intelligence.	Limited to structured COTS watchlist with Dow Jones or World-Check services or from governmental sites like OFAC or EU sanctions.
Advantage Does not rely solely on COTS watchlists, enables investigators to enrich the source datasets.	**Advantage** None.
Disadvantage None.	**Disadvantage** Limitation to the above-mentioned sources. More restricted investigative capability.

Company Profile

idetect® is a next generation software for Enterprise Fraud, Anti-Money Laundering, Transaction Monitoring, Know-Your Customer (KYC) and Client Onboarding, and Watchlist Monitoring, which provides the latest and most efficient technological features against financial crime and illicit transactions.

LOGOS ITS S.A., a company based in Luxembourg and Germany, is the editor and distributor of the technology. Our company delivers high-quality services and solutions for market leaders in the area of finance, industry, and government. With 20 years of experience and an average of 65 highly skilled employees in the 3 last years, the reliability and stability of the team has allowed to collaborate, establish partnerships and official agreements with some of the largest institutions in Europe and the World.

LOGOS ITS has numerous prestigious clients among which Agricultural Bank of China (ABC), China Merchants Bank (CMB), Crédit Agricole-Caisse d'Épargne Investor Services (CACEIS), Banque et Caisse d'épargne de l'État Luxembourgeois (BCCE), Arcelor Mittal, LuLu International Exchange, Bahrain Financing Company, Wafacash, CIHBank, Swisscard and Deutsche Börse Group (Clearstream Services, Regis-TR, Deutsche Börse Security Services, Eurex).

Our company is also investing heavily into research and innovation including a specific partnership framework with the Science University of Luxembourg and the Ministry of Economy. Researches focus on machine-learning and artificial intelligence to combat financial crime.

Contact us at:
info@idetect-soft.eu | +352 26 36 55-1

idetect