AML Management:

Challenges and Opportunities

FISER CONSULTING
FINANCIAL SERVICES

Contents

Introduction

Back in August 2011, HSBC suffered from having business relations with Mexican "Cartels". The sustainability of HSBC was jeopardised, which is why other Financial Institutions started to invest in programs to implement controls and technologies to prevent such incidents. Seven years later, and after a great scrutiny by global and local regulators, Financial Institutions have not cleared the trial. In February 2017, Rabobank was charged with involvement in misconducts committed with drug cartels.

Money Laundering is a direct threat to the long-term sustainability of any business. In the eyes of the regulators, Anti Money Laundering (AML) is critical because it compromises a company's image and reputation. Regulators have shown little patience with Financial Institutions that lack the internal controls and that have engaged in business relationships with clients that are involved in criminal activities.

However, the cost of implementing an effective compliance program is expected to increase[1] in the following years. This puts pressure on compliance departments to protect institutions because they have less resources available that can lead to compliance gaps and ultimately expose institutions to AML risk. The management must take a closer look at the current processes and activities that constitute the "AML Management Cycle", to detect bottlenecks, process gaps and overall inefficiencies.

The "AML Management Cycle" is defined as 'all activities and processes that are executed by a Financial Institution to mitigate the risk of Money Laundering'. The cycle has four stages which are (1) Client onboarding, (2) Customer Due Diligence (3) Customer Monitoring and (4) Case Management. The organisation's AML Management Cycle provides a blueprint of the operational flow of the AML unit which is fundamental to improve operations.

Other additional challenges of the AML Management Cycle that Financial Institutions are facing are side effects of technological developments, regulation and financial globalisation. First, the implementation of sophisticated transaction monitoring systems has caused an excessive increase in the number of false-positive alerts, which are timely and costly to Institutions. Second, the identification of the Ultimate Beneficial Owner (UBO) is a lengthy and complicated process. Third, Financial Institutions have been growing their customer base in developing and emerging economies which led to a significant risk in engaging with forbidden business relationships.

Top Financial Institutions paid over 4.198 million euros in fines due to AML penalties from 2010 to 2017. These sanctions were examined and placed in a phase of the AML Management Cycle. The analysis was made to identify the significant operational pitfalls incurred in the past and to provide exciting insights to prevent future obstacles.

To solve the situations listed above, Financial Institutions are looking for innovative technologies to evolve Compliance from an operational to a strategic function. In this paper three success stories are presented on how leading Financial Institutions increased their security barriers for client authentication using biometrics, how they improved operational processes using AI and a how they distributed ledger technology (blockchain) to secure payments.

As a niche consultancy firm, FiSer Consulting finds it important to define strategies that equip Financial Institutions with capabilities to solve regulatory issues and to maximise value for the application and processes to mitigate the AML risk.

[1] Accenture (2017) Compliance: Dare to be Different retrieved from: https://www.accenture.com/us-en/insight-compliance-risk-study-2017-financial-services

Stages of AML Management Cycle

The "AML Management Cycle" has four principal stages. First, a company must know the identity and economic activity of the client during the onboarding phase. This knowledge depends on the regulatory framework where Financial Institution locate their customers need to present specific documentation, e.g. valid passport, identity card, etc. Currently, "all digital banks" such as Bunq Bank conduct this process by requesting clients to send a picture of their documentation and to conduct a short online interview with a customer service representative[2].

Second, Financial Institutions must gather, safeguard and continuously update relevant identity and financial documentation to integrate a full client record. This process is called Know your Customer (KYC). Third, a transaction monitoring system (AML) must be in place to review that each of the transactions operated by the customers corresponds to the customer's transactional profile and that it identifies "alerts" for each transaction that seems unusual. A fourth point states all suspicious transaction that represent a real threat to the institution are subject to further review.

The Compliance Analysts that operate the transaction monitoring process execute extensive due diligence on the customer identity and the customer's business relations (essential clients, stockholders, suppliers) for each alert presented. The analysis and documentation of an alert can take up to 45 minutes[3]. To simplify this process, Financial Institutions are creating strategic alliances with each other to share information and to detect suspicious behaviours in a more efficient and timely manner to the correspondent parties[4].

Moreover, the irregular transactions that represent a real threat to the institution are subject to a supplementary examination. The Case Management phase is the "second" analysis that the Compliance Analyst performs. At this stage the Analyst decides to cancel the account or dismiss the client. Each decision must be approved by the Risk Management Committee.

The AML Management Cycle requires an integrated IT infrastructure that not only supports and assists the Compliance Analyst in their due diligence but also consolidates the information and presents it across businesses and products. There are several solutions in the market (SAS, Norkom, Oracle, to name a few) that follow this methodology. However, the challenge that most institutions face is to build an accurate "one" view report per client[5]. Figure 2, shows the evolution of these processes and explains some relevant activities that happen at each stage.

Finally, a Policy should exist that merges local and global standards with specific business characteristics and corporate guidelines. This policy would dictate the rules and guidelines of the AML prevention unit.

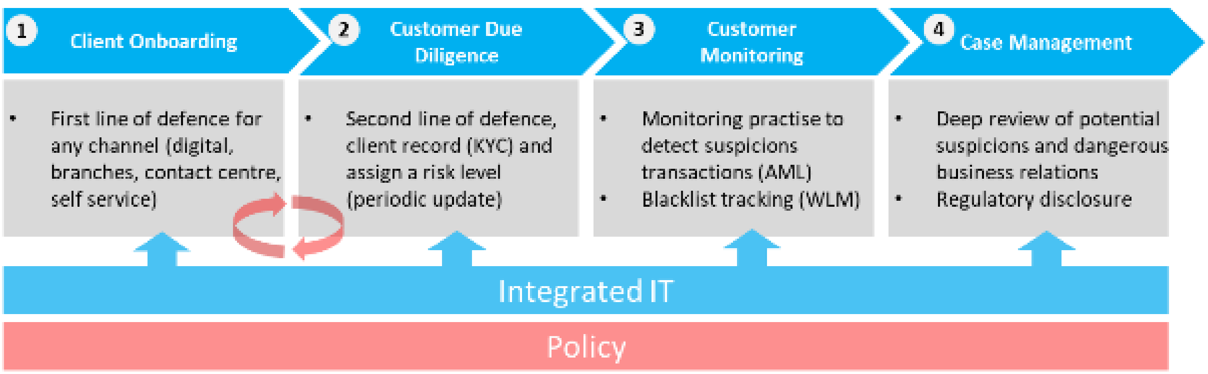

Figure 1.- AML Management Cycle

---

[2] Deloitte US (2017) Deloitte Digital Bank – Customer Onboarding retrieved from https://www.youtube.com/watch?v=IoQqchI0A-k&t=4s
[3] Domino Advisory (2017) Transaction Monitoring Alerts: The Source of AML Compliance Failure retrieved from http://www.dominion-advisors.com/blog/transaction-monitoring-alerts-the-source-of-aml-compliance-failure/
[4] Slater (2014) Six banks team up in plan for shared customer data register retrieved from https://www.reuters.com/article/us-banks-compliance-register/six-banks-team-up-in-plan-for-shared-customer-data-register-idUSBREA2319120140304
[5] Khosla (2016) Regulatory Compliance and Customer Centricity: Can Banks address both? https://www.pega.com/insights/articles/regulatory-compliance-and-customer-centricity-can-banks-address-both

Current challenges

Excessive false-positive alerts

Financial Institutions have implemented Transaction Monitoring Systems (TMS) to automate the tracking and detection of AML activity of their clients. The TMS systems has two objectives: (1) detect unusual financial transactions and (2) certify the compliance with official blacklists.

1. Detect unusual financial transactions

The TMS is connected with a client database which contains the "transactional profile" of the customer-defined during the KYC. The transactional profile is a predefined limit of amounts and quantity of funds that a client can operate in a period. The TMS creates an alert each time that one of the transactions exceeds the defined threshold. Later a compliance analyst reviews each signal to determine its relevancy.

2. Certifying compliance with official blacklists.

Financial Institutions need to guarantee their clients, correspondent banks, UBO and other non-customers entities (stakeholders) that they are not involved with AML activities. Financial Institutions will need to ensure that they are compliant with official blacklists. If a stakeholder's information (name and birth) "match" with the person listed on the blacklist, an alert is created. Financial Institutions periodically compare the stakeholder's name, date of birth and nationality with the blacklist released by global organisations such as:

- Office of Foreign Assets Control (OFAC)
- Federal Bureau of Investigation (FBI)
- Central Intelligence Agency (CIA)
- EU terror list
- INTERPOL and EUROPOL
- Local Blacklist depending on the country were the business relation is based

The two processes outlined above, generate a lot of fake alerts, better known as "False-Positives". The false positives are estimated to constitute almost 90% of all the total alerts[6]. This situation represents one of the first challenges that Financial Institutions are currently facing - time and resources. The Customer Monitoring process has the most significant amount of headcount and allocated resources within the AML Cycle. The Financial Institution that brings more accuracy to the TMS will outperform the market.

Verification of Ultimate Beneficial Owners (UBO's)

The process of the UBO identification happens during the client onboarding for wholesale clients. Financial Institutions need to certify that the wholesale customers are not partially or entirely owned or manipulated by suspicious individuals or entities.

The Ultimate Beneficial Owners (UBOs) is a physical person that has relevant equity participation in a company's capital structure. According to the EU AMLD4 and the US FinCEN framework UBOs has three primary characteristics:

1. Natural person who holds 25% plus one share of the company
2. Or person(s) that exercises control over the management of a legal entity
3. Or person(s) that holds a position of senior managing official (CFO, CEO, VP, Treasurer etc).

[6] Dow Jones Acams (2016) GLOBAL ANTI-MONEY LAUNDERING - SURVEY RESULTS 2016 retrieved from http://files.acams.org/pdfs/2016/Dow_Jones_and_ACAMS_Global_Anti-Money_Laundering_Survey_Results_2016.pdf

Tax compliance regulations such as FATCA, have introduced a requirement for a 10% threshold for beneficial ownership (US citizen), which is significantly higher than the 25% norm. This adds additional pressure to the policy of the onboarding process.

The challenge of UBO identification lies in the lack of clarity in the financial structure of the company. It is common that global conglomerates have complex ownership structures that flow through different subsidiaries. This situation creates bottlenecks during the onboarding process.

Cross border AML management

Global Financial Institutions find it challenging to enforce corporate controls over the branches located in countries with different compliance rules. During 2016 several Financial Institutions were considering exiting an existing business line or correspondent banking relationship due to regulatory risk. This phenomenon is called *de-risking* where Financial Institutions terminate or restrict business relationships with clients or categories of clients to avoid risk in line with AML[7].

Moreover, several Financial Institutions have seen a decline in correspondent banking relationships, which brings a substantial impact to the availability of funds and money flow in the global banking landscape. This has led to an increasing demand for less regulated channels such as money remittance services. The growing pace of this trend is alarming because the deterioration in the number of correspondent banking relationships will affect the ability to send and receive international payments[8].

However, some Banks are taking actions to mitigate the risk of deterioration of correspondence relationships. For example, Standard Chartered has released a correspondent banking training program in 23 Asian countries to help its clients, local banks and their client's clients to comply with AML Rules[9].

Operational pitfalls

From 2010 to 2017, 21 of the most significant banks in Europe had to pay a fine of approximately 4,198 million euros. The details of each fine and sanctions per Financial Institution is presented in the table below. Information from relevant newspapers and news sites were used for this analysis.

Based on the table, it can be concluded that Financial Institutions showed to be most fragile in Customer Due Diligence (CDD). CDD alone accounts for 3,019 million euros in fines, followed by the Client Onboarding process with 588 million euros in fines and finally, Transaction Monitoring with respectively 253 million euros in fines. Some institutions presented overall mismanagement and problems while enforcing a global AML policy; these pitfalls lead to 338,3 million euros in fines.

[7] Alani (2017) De-Risking 'Phenomenon' Puts 700 Million Globally at Risk retrieved from https://www.brinknews.com/de-risking-phenomenon-puts-700-million-globally-at-risk/
[8] Taylor (2017. De-Risking and Financial Inclusion retrieved from http://www.acamstoday.org/de-risking-and-financial-inclusion/
[9] Adriano (2017) When Money Can No Longer Travel retrieved from http://www.imf.org/external/pubs/ft/fandd/2017/06/adriano1.htm

Bank	Approx. fine	Sanction motive	Process affected	Period
Banco Santander	1 million EUR	Relationship with Group Rumasa [(1)]	Customer Due Dilligence	2016
Barclays Bank	88 million EUR	Insufficient CDD/KYC for High Risk Clients and PEPs [(2)]	Client Onboarding	2015
BBVA	500 million EUR	Executives of BBVA involved in the Forex case in Paraguay [(3)]	Client Onboarding	2016
BNP Paribas	10 million EUR	Insufficient staff and tools for transaction monitoring [(4)]	Transaction Monitoring	2017
BNP Paribas	7 million EUR	Violated US sanctions related to Iran, Sudan and Cuba [(4)]	Customer Due Dilligence	2014
Commerzbank	1,000 million EUR	Violated US sanctions related to Iran, and other sanctioned countries [(5)]	Customer Due Dilligence	2015
Credit Agricole	655 million EUR	Violated US sanctions related to Iran, Sudan, Cuba and Myanmar [(6)]	Customer Due Dilligence	2015
Credit Suisse	13 million EUR	Deficient tools and process for transaction monitoring [(7)]	Transaction Monitoring	2016
Deutsche Bank	34 million EUR	Failed to comply with BSA and ineffective transaction monitoring [(8)]	Transaction Monitoring	2017
HSBC	34 million EUR	Inadequate AML-unit organisation in a Swiss branch [(9)]	Overall process and global policy	2016
ING	Not settled	Collusion with high-risk clients in Uzbekistan [(10)]	Client Onboarding	2017
Intesa Sanpaolo	195 million EUR	Failed to detect transactions with Iran [(11)]	Transaction Monitoring	2016
Nordea	5 million EUR	Insufficient CDD/KYC and transaction monitoring process [(12)]	Customer Due Dilligence	2016
Rabobank	298 million EUR	Involvement with Mexican Drug Cartels [(13)]	Overall process and global policy	2017
RBS	6 million EUR	Ineffective CDD/KYC and transaction monitoring NatWest, Ulster Bank and Coutts[(14)]	Customer Due Dilligence	2010
RBS - Coutts	7 million EUR	Ineffective CDD/KYC and monitoring processes [(15)]	Customer Due Dilligence	2017
Societe Generale	5 million EUR	Insufficient AML controls after ACPR audit [(16)]	Overall process and global policy	2016
Standard Chartered	283 million EUR	Violated US sanctions related to Iran [(17)]	Customer Due Dilligence	2014 - 2016
UBS	800 K EUR	Inadequate AML controls in a Singapore branch [(18)]	Overall process and global policy	2016
Unicredit	Not settled	Violated US sanctions related to Iran [(19)]	Customer Due Dilligence	2012 - 2016

(1) Reuters (2016) Banco Santander fined 1 mln euros for failing to stop money laundering retrieved from https://www.reuters.com/article/santander-fine/banco-santander-fined-1-mln-euros-for-failing-to-stop-money-laundering-idUSL8N1DT2TI
(2) FCA (2015) FCA fines Barclays £72 million for poor handling of financial crime risks retrieved from https://www.fca.org.uk/news/press-releases/fca-fines-barclays-%C2%A372-million-poor-handling-financial-crime-risks
(3) Lavanguardia (2016) Primeras condenadas en caso por lavado de 600 millones de dólares en Paraguay retrieved from http://www.lavanguardia.com/vida/20160902/4173999884/primeras-condenadas-en-caso-por-lavado-de-600-millones-de-dolares-en-paraguay.html
(4) Reuters (2017) BNP Paribas fined over weaknesses in anti-money laundering controls retrieved from https://www.reuters.com/article/us-bnp-paribas-moneylaundering/bnp-paribas-fined-over-weaknesses-in-anti-money-laundering-controls-idUSKBN18T2JI
(5) Cassin (2015) Compliance fiasco: Commerzbank pays $1.45 billion for AML, sanctions, and fraud-related offenses retrieved from http://www.fcpablog.com/blog/2015/3/12/compliance-fiasco-commerzbank-pays-145-billion-for-aml-sanct.html
(6) Chon & McLannahan (2015) Crédit Agricole pays $787m penalty for busting US sanctions retrieved from https://www.ft.com/content/2dcf96e2-7744-11e5-a95a-27d368e1ddf7
(7) Condon (2016) FINRA Fines Credit Suisse Securities (USA) LLC $16.5 Million for Significant Deficiencies in its Anti-Money Laundering Program retrieved from http://www.finra.org/newsroom/2016/finra-fines-credit-suisse-165-million-significant-deficiencies-its-aml-program
(8) Hamilton & Arons (2017) Deutsche Bank Fined $41 Million for Money-Laundering Lapses retrieved from https://www.bloomberg.com/news/articles/2017-05-30/deutsche-bank-pays-41-million-fine-for-money-laundering-faults
(9) Martin (2017) HSBC faces FCA probe into anti-money laundering controls as profits plunge retrieved from http://www.telegraph.co.uk/business/2017/02/21/hsbc-profits-slump-volatile-year/
(10) Meredith (2017) ING faces money-laundering and corruption probe retrieved from https://www.cnbc.com/2017/03/22/ing-faces-money-laundering-and-corruption-probe.html
(11) Freifeld (2016) New York regulator fines Italy's Intesa Sanpaolo $235 million retrieved from https://www.reuters.com/article/us-intesa-fine/new-york-regulator-fines-italys-intesa-sanpaolo-235-million-idUSKBN1442A8
(12) Reuters (2005) UPDATE 1-Nordea, Handelsbanken fined over money laundering breaches retrieved from https://uk.reuters.com/article/nordea-bank-handelsbanken-fsa/update-1-nordea-handelsbanken-fined-over-money-laundering-breaches-idUKL5N0YA1MS20150519
(13) Jan Eijpe (2018) Rabobank, National Association settles compliance program matters retrieved from https://www.rabobank.com/en/press/search/2018/20180207-rna.html
(14) Wray (2010) RBS handed FSA's biggest fine for lapses over money laundering rules retrieved from https://www.theguardian.com/business/2010/aug/03/royal-bank-of-scotland-fsa-biggest-fine
(15) Katz & Miller (2017) Queen's bank Coutts fined by Swiss financial regulators over money laundering retrieved from http://www.independent.co.uk/news/business/news/coutts-ban-fines-queen-swiss-financial-regulators-money-laundering-switzerland-illegal-profitting-a7559716.html
(16) Reuters (2017) French bank watchdog fines SocGen 5 million euros over anti-money laundering shortcomings retrieved from https://uk.reuters.com/article/uk-socgen-moneylaundering/french-bank-watchdog-fines-socgen-5-million-euros-over-anti-money-laundering-shortcomings-idUKKBN1A626Z
(17) White and Barlyn (2016) StanChart faces extension of U.S. money-laundering vigilance retrieved from https://uk.reuters.com/article/uk-hsbc-stanchart-compliance/stanchart-faces-extension-of-u-s-money-laundering-vigilance-idUKKCN118223
(18) Rahman (2016) Singapore's MAS tells Falcon to close, fines DBS, UBS over 1MDB retrieved from https://www.cnbc.com/2016/10/10/singapores-mas-tells-falcon-to-close-fines-dbs-ubs-over-1mdb.html
(19) Reuters (2015) UniCredit in 'constant talks' with U.S. authorities over Iran probe: CEO retrieved from https://www.reuters.com/article/us-unicredit-ceo/unicredit-in-constant-talks-with-u-s-authorities-over-iran-probe-ceo-idUSKBN0M917O20150313

Table 1.- AML fines per Top European Bank

A more in-depth understanding of the causes that originated the sanctions is provided as follow:

Under the process of Customer Due Diligence, Financial Institutions:

- Failed to conduct basic CDD. - This situation occurs when the Financial Institution is unable to carry out adequate background checks and screening processes for clients. For example, Switzerland's financial regulator received a fine from Coutts & Co (RBS subsidiary) for allowing 1Malaysia Development Berhad (high risk customer) transfer funds to a Swiss account. 1Malaysia Development Berhad started a relationship with Coutts & Co in 2009.

- Violated US sanction with banned countries. - Financial Institutions that held business relationships and transactions with prohibited countries have accumulated fines of approximately 1,499 million euros. While the OFAC (US) recognises high-risk 30 nations, the FinCEN (US) has a much broader scope with 50 countries[10]. In general, Financial Institutions found difficulties in cutting ties with companies located in Iran, Sudan, and Cuba.

For the Client Onboarding process, Financial Institutions received fines for:

- Collusion with forbidden customers. - This situation happens when internal staff collaborate with prohibited clients to transfer resources, hold accounts and use financial services. This case must be treated with delicacy because it

[10] Sanctions wiki (2011) US Embargoed Countries http://www.sanctionswiki.org/US_Embargoed_Countries

constitutes a critical offense to the integrity of the Financial Institution. These situations are hard to control because they involve internal staff collaboration and agreement.

- Insufficient controls for KYC requirements. - Financial Institutions fail to gather and update client's information also missed identifying the source of funds and PEP (Political Exposed Person) business participation.

Financial Institutions that failed in the Overall process and global policy implementation presented two significant difficulties:

- Global Policy enforcement and controls. - This stage of the overall process represents the implementation of AML corporate policies at international branches. Financial Institutions have found difficulties to manage risk outside the boundaries of their home country. For example, Rabobank was accused of collaboration with Mexican drug cartels which harmed the Institution with a 298 million euros fine and a substantial decrease in the bank's global reputation.

- Overall inadequate AML controls. - After an audit conducted by ACPR, Société Générale received a fine of 10 million euros for having insufficient AML controls. The high fine shows that that the institution failed to implement an affirmative AML management cycle across the financial group.

Financial Institutions that failed to detect suspicious transactions had to pay 253 million euros in fines. This shows that such transactions are a common pitfall for Europe's most significant Banks. For example, in 2016, FINRA fined Credit Suisse for 13 million euros (USD 16.5 Million) for having a deficient suspicious transaction monitoring program. The regulator pointed out that Credit Suisse's monitoring program was inadequate in two aspects: (1) It failed to investigate and escalate the high-risk activity detected and (2) its automated surveillance system for monitoring suspicious money transactions was inadequately implemented[11].

Table 2 shows the process gap detail for each AML management cycle.

Faulty Process	Process Detail	# Cases	Approx. fine million euros
Customer Due Diligence	Failed to conduct basic CDD	5	1,520.00
	Violated US sanctions with banned countries	5	1,499.10
Client Onboarding	Collusion with client	2	500.00
	Inadequate controls and KYC	1	88.00
Overall process and global policy	Global policy enforcement and controls	3	333.30
	Inadequate overall anti-money laundering controls	1	5.00
Transaction Monitoring	Failed to detect suspicious transactions	4	253.00
Total		21	4,198.40

Table 2.- Detailed process gaps

[11] Condon (2016) FINRA Fines Credit Suisse Securities (USA) LLC $16.5 Million for Significant Deficiencies in its Anti-Money Laundering Program retrieved from http://www.finra.org/newsroom/2016/finra-fines-credit-suisse-165-million-significant-deficiencies-its-aml-program

Closing the gap – Success stories

The previous sections of this paper showed that managing AML is a challenging task that requires strict control. However, some Financial Institutions are looking to innovative technology to increase the security level of the entire cycle and to provide the Compliance function with strategic tools.

The following section provides an analysis of three case studies that explain the implications of implementing an emerging technology in the AML Management Cycle. Figure 2 shows the place where an emerging technology such as Biometrics, AI and Blockchain will impact at the AML Management Cycle. During the client onboarding phase, the use of Biometrics as a mean of customer authentication can be beneficial. Moreover, AI can be implemented in the Transaction Monitoring process to reduce false positives. Finally, Blockchain technology can change the money remittance business for good by providing transparency.

Biometrics – the next step in KYC management

On April 2017, Mastercard disclosed a new generation of cards that merge chip technology with fingerprints to increase the security in the customer authentication process. This initiative was released in South Africa with Pick n Pay, Absa Bank, and Barclays.

The biometric application represents changes in the Client Onboarding process. Cardholders provide their fingerprint during onboarding. At a later stage, the Bank creates a digital template with encrypted prints linked to the card. The card is then ready for use at any EMV (Europay, MasterCard, VISA) card terminal. Each time the client uses the card, the merchant validates the transaction asking the customer to place their fingers on a sensor to approve the operation[12].

The above case represents a perfect example of the digital transformation of KYC requirements. The biometric technology is a reliable ally to prevent fraud, to increase approval rates, and to gain customer loyalty.

Artificial Intelligence – Reinvention of the compliance function

HSBC has been affected by money laundering on several occasions. In the last ten years, the bank has had over 1,928 million euros in fines. The most critical scandals were in 2012, when the institution failed to maintain an adequate program against AML in Mexico. Still, in 2017, HSBC swiss branch allowed money laundering due to organisational inefficiencies.

However, HSBC has currently reinvented itself as a technology leader and has partnered up with Ayasdi, an US-based artificial intelligence start up to automate a couple of AML investigation processes[13]. In a twelve-week period, Ayasdi's was able to achieve a 20 percent reduction in false positives while maintaining the same number of reports to case management[14].

Ayasdi designed an AML solution that automatically creates categories between customers and third-party relations, allowing the Compliance Analysts to build distinctive scenarios and rules for each bucket. This categorisation enables the institution to balance between "signal and noise", meaning: the reduction of false positives[15]. HSBC is an excellent example of innovation and self-reinvention.

Blockchain – Free money transfer

Blockchain architecture is a subtype of a centralised ledger comprised of multiple digitally recorded data, such as transactions agreements and settlements. Blockchain spreads incoming information across an extensive network of computers around the world.

---

[12] Mastercard (2017) Thumbs Up: Mastercard Unveils Next Generation Biometric Card retrieved from https://newsroom.mastercard.com/press-releases/thumbs-up-mastercard-unveils-next-generation-biometric-card/

[13] Ayasdi Team (2017) Anti-Money Laundering and AI at HSBC retrieved from https://www.ayasdi.com/blog/financial-services/anti-moneylaunderinghsbc/

[14] Moore-Colyer (2017) HSBC Adopts AI Startup Ayasdi's Tech To Tackle Money-Laundering retrieved from http://www.silicon.co.uk/data-storage/bigdata/hsbc-ai-ayasdi-213717?inf_by=5a339d6e681db88a748b46c1

[15] Ayasdi (2017) ANTI-MONEY LAUNDERING Don't Change Rules, Change the Game retrieved from https://www.ayasdi.com/solutions/anti-money-laundering/

The blockchain technology can be utilised in international money transfers because its distributed database allows direct communication between users and transparency in operations. Additionally, blockchain technology permits the users to set up their rules and it automatically trigger transactions.

The above characteristics make Blockchain perfect to develop applications that improve the flow of money across geographies. The money remittance industry had a value of $429 billion in 2016[16]. Currently, Financial Institutions charge an average of 7.45% in fees per transaction; in some developing economies transactions fees can be up to 15 %[16].

Circle is a company that capitalised the above opportunities in the international money transfer industry. The company builds its application in Ethereum and currently allows customers to send payments between geographies using their mobile phones. In 2016 the company processed over $1 billion in transactions[17].

The transparency of Blockchain technology reduces the risk of AML allowing the users with a pseudonym the possibility of tracking each transaction. Circle is not the only company that is changing the remittance industry. Other relevant examples are Abra, Align Commerce, Bitspark, Coins.ph, Rebit, CoinPip, Hellobit, TransferB, BitPesa, Romit and Volabit[18].

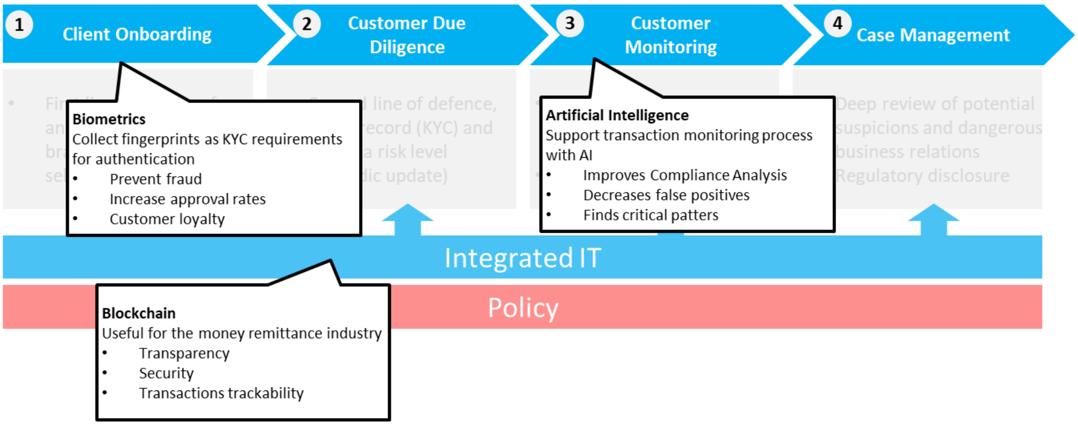

Figure 2.- Impact of Technology into AML Management Cycle

[16] Schiller (2017) The Fight For The $400 Billion Business Of Immigrants Sending Money Home retrieved from https://www.fastcompany.com/3067778/the-blockchain-is-going-to-save-immigrants-millions-in-remittance-fees
[17] Reuters (2017) Blockchain start-up Circle launches a no-fee international currency exchange retrieved from https://www.cnbc.com/2017/06/15/circle-launches-an-international-money-transfer-service.html
[18] Amit (2015) 11 Money Transfer Companies Using Blockchain Technology retrieved from https://letstalkpayments.com/11-money-transfer-companies-using-blockchain-technology-2/

How can we help

As a niche consultancy firm, FiSer Consulting finds it essential to define strategies that equip Financial Institutions with the capabilities to solve regulatory issues and to run smooth and efficient AML operations. The most critical element that Financial Institutions need to tackle is in the first place the design of internal policies that are aligned with the global and local regulatory frameworks. Second it also needs to enforce those policies in everyday operations.

Policy level advisory

An adequate AML program must consider an internal policy that recognises four elements which are (1) Local Regulatory Frameworks, (2) Global Standards (3) Specific Business Activities and (4) Corporates Guidelines. Figure 3 provides examples of a local policy structure, which keep Local and Global Standards as central position. Additionally, the internal policy must be specific and suitable for the business activity and corporate guidelines of the Institution.

It is crucial that the AML policy remains updated with the current regulatory reforms. An example occurred back in December 2017 when the European Parliament and the European Council came to an agreement related to the amendments made to the Anti-Money Laundering Directive (AMLD 5).

AMLD5 will introduce stricter rules for financial flows from high-risk countries, it will mitigate risks linked to virtual currencies, and provide transparency when it comes to UBOs from large corporations.

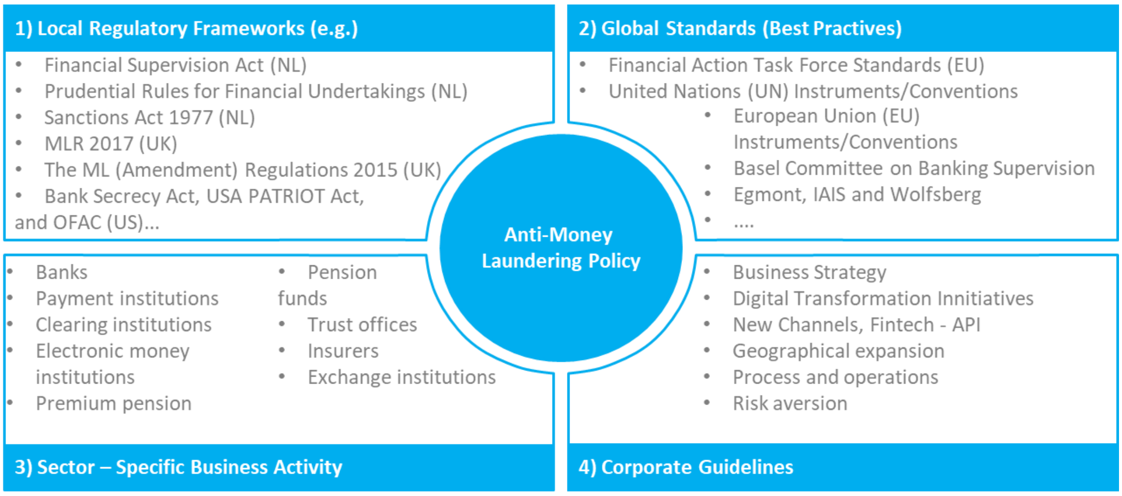

Figure 3.- Dimensions AML Policy

AML management cycle improvement

Economic success depends on the control of processes, while a lack of control will give rise to inefficiencies. This paper has highlighted that exponential increase of workloads due to excessive regulation and asymmetry in transaction monitoring systems produces excessive false-positive alerts. These alerts are the main concern and issue in the AML management cycle.

FiSer Consulting can provide a precise diagnostic of the operational pitfalls in the AML management cycle. This diagnosis can help the organisation to detect risks and functional inefficiencies that can lead to business unit transformation, implementation of an emerging technology or a process re-engineering program. The decisions during the diagnostic will be derived from the analysis of relevant data with the objective of improving the communication, risk management and resources involved in the AML management cycle. Figure 4 shows the three phases of the improvement cycle and the strategic directions of the initiative.

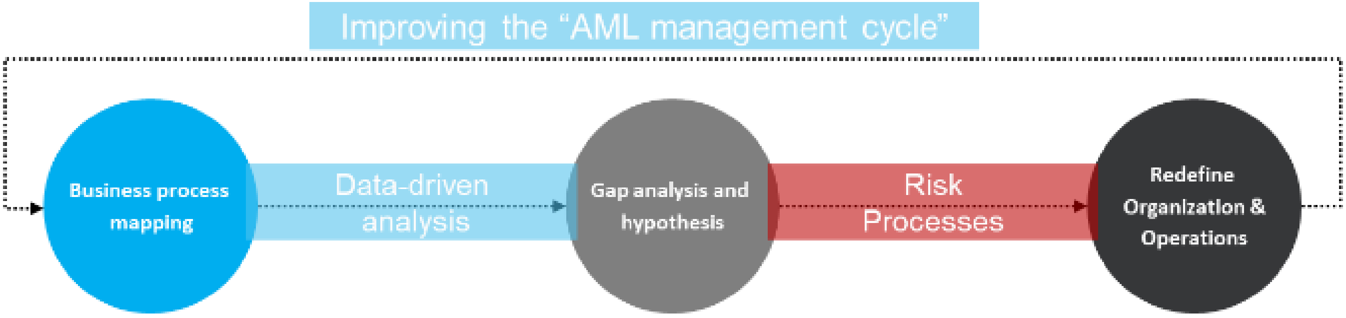

Figure 4.- Transformation of AML Unit

Each phase includes the following activities:

Business process mapping

- Identification of the relevance of each process in the "AML management cycle."
- The collection of relevant indicators and metrics, e.g. number of alerts originated in the Branch network, number of cases, headcount per process, time per alert, etc...
- Categorisation of processes by risk sensitivity and operational impact
- Engagement in interviews with relevant stakeholders
- Conduction of process documentation and analyse significant activities

Gap analysis and hypothesis

- Identification of meaningful bottleneck and operational issues
- Verbalization of the hypothesis and test solutions
- Categorisation of the successful hypothesis which depends on complexity, e.g. quick wins or long-term implementations

Redefine Organization & Operations

- Development of strategic analysis and a roadmap for implementation
- Altering or adding changes in operating models and organisation
- Monitoring changes and compare metrics

Glossary of terms

Term	Definition
1MDB	1Malaysia Development Berhad
AML	Anti-Money Laundering
AMLD4	4th EU Money Laundering Directive
BIS	Bank of International Settlements
BSA	Bank Secrecy Act
EMV	Europay, MasterCard, VISA
FinCEN's	Financial Crimes Enforcement Network
FATCA	Foreign Account Tax Compliance Act
FINRA	Financial Industry Regulatory Authority
US	United States of America
ACPR	Autorité de contrôle prudentiel et de résolution

Next steps

For further information, please contact:

FiSer Consulting | Dirk Worm

Dirk has over 20 years of experience in Global Financial Markets, particularly in the Investment Banking and Corporate & Commercial Banking industries. Dirk's consulting skills lie in risk management, capital management, front office transaction management, the implementation of asset & liability management and treasury functions, and the implementation of regulatory processes, including Basel II, III, MiFID and EMIR.

Contact: d.worm@fiser.consulting

FiSer Consulting | Roberto Nieves

Roberto has over 5 years of experience as management consultant, leading and promoting innovation for top financial institutions. Roberto's consulting skills are mostly in transformation management, business strategy, and compliance implementation with a deep understanding of wholesale banking.

Contact: r.nieves@fiser.consulting

Barbara Strozzilaan 201
Tel.: +31 20 20678386
1083 HN Amsterdam
www.fiser.consulting
The Netherlands