RT ASSOCIATES

AML - A New Era

How to achieve a leading approach to managing AML

Author : Dr Sian Lewin

November 2020 | RegTech Associates

Foreword

by Matthew Redhead, Associate Fellow at RUSI

Now, more than ever, we need to improve how we tackle money-laundering and financial crime. I'll explain why - when we consider anti-money laundering, there are two sides to the issue - how criminals and the modern criminal economy works and how our efforts to deal with the criminal economy are framed in response.

Criminals clearly don't publish their key performance measures but reliable estimates suggest between 2% and 5% of global output per year can be attributed to the proceeds of crime[1]. Based on 2019 global output figures, that indicates somewhere between $1.7 and $4.3 trillion is illicitly obtained in any given year.

So why are the criminals doing so well? Increasing globalisation, the massive shift to digital channels for finance and gambling, the emergence of crypto assets as well as peer-to-peer platforms provide criminals with a whole range of new ways to launder their illicit gains, on top of the more traditional methods such as cash smuggling and trade-based money laundering.

Huge amounts of money are being laundered each year, by increasingly sophisticated and complex methods employed by savvy criminals making the most of new and innovative technologies.

How are we doing in response? Well, if we go back to the statistics, the criminals are doing a lot better than we are. Europol estimates that less than 2% of criminal assets are recovered[2]. That's a remarkably small amount given how much is invested by the public and the private sector in fighting financial crime.

Why is this the case? I think there are two main reasons. Firstly, the AML framework that has developed over the last three decades is relatively static but financial criminality develops and grows like an organism, constantly testing the boundaries and coming up with new ideas.

Secondly, the framework is fragmented - in financial institutions, AML departments have grown, becoming increasingly specialised to meet the growing detailed requirements of regulatory demand. As they become more specialised, they become delinked and decoupled from each other. They exist in their own stovepipes, not in the complex web of interaction that we see in the criminal world.

Better integration has to be a critical aim for all anti-money laundering professionals, both in the public and in the private sector. There is plenty that individual institutions can still do now to improve the situation now - it's increasingly feasible for an individual financial institution to pool its own internal data, integrate systems and provide themselves with a better, more holistic, 360 degree view of their clients, which makes it much easier to judge the potential AML and financial crime risks.

But it's not just feasible, it's also a matter of corporate social responsibility. Financial criminals operate in the gaps that we create for them. We've created many gaps with the system so far, and I would suggest it's therefore our responsibility as AML professionals to try and find ways in which to close those gaps in the future.

About Matthew

Matthew Redhead is a researcher and writer on financial crime and national security topics, and an independent risk consultant to the FinTech and RegTech sectors. He is also a regular contributor to Jane's Intelligence Review on serious organised crime, financial crime, terrorism and intelligence. He has extensive experience in financial services, having trained as a 'front office' banker for HSBC in the 1990s, and worked there for the last seven years in various senior roles in the financial crime risk function, his last role being Global Head of Strategic Intelligence. He has also served as a government official at the MoD, and on secondment at the Office of Security and Counter-Terrorism (OSCT) at the Home Office.

Introduction

> Financial criminals operate in the gaps that we create for them

In our conversations with anti-money laundering practitioners, technology vendors and industry experts, it has become clear that there is a common desire to 'do better' in fighting financial crime. Considering the human cost and suffering that sits behind financial criminality is a huge motivating factor for the financial industry but doing better and the associated transformation that it involves can be difficult. In Part 1, we explore current AML capabilities and approaches, recognising both the challenges and why now is the time to act.

In our view, firms really need to ask difficult questions about the reality of their current AML capabilities and take stock of where they are and then where they need to get to is critical to enable firms to improve their AML capabilities and work towards having a leading approach. In Part 2, we have collaborated with Napier, a London-based AML technology vendor to understand how the maturity model they have created based on their experience with customers, offers a series of concrete targets to aim for to level up to leading AML capabilities.
Technology clearly plays a huge part in this journey towards this leading level of AML, but in a crowded market, how do you navigate this fog of innovation?

Really understanding where you are and the specific problem you are trying to solve is obviously critical - but then ensuring you choose technology with a nod to the future is also important. This avoids firms having to continually overcome the current challenges of legacy technology - and legacy thinking - again in ten or fifteen years time. Most importantly, plotting the journey to achieving a leading level of AML capabilities requires senior management commitment and a shift in culture and mindset. Without this, financial criminals will continue to evade justice and the real price will be paid in human suffering and harm.

PART 1: THE STATE OF PLAY

How do regulated firms currently fight financial crime?

It is fair to say that the current approach to fighting financial crime is largely influenced by the regulatory framework, cascading from the Financial Action Task Force recommendations down to national legal frameworks and regulatory guidance. One of the most consistent requirements is that firms should use a risk-based approach to managing financial crime compliance - an approach where resources (time and effort) are allocated to customers, products and transactions that pose the highest risk of financial criminality. Despite this ambition, most financial institutions would admit they are falling short of this ideal.

Research by McKinsey[3], for example, indicates that when it comes to customer risk ratings, most models identify between 0 and 5% of the entire customer base as being potentially high risk and therefore requiring enhanced due diligence. For the remaining 90+%, they may be grouped in as few as one or two segments and therefore similar levels of resources are allocated to dealing with customers that are actually at quite different levels of risk.

In other parts of the AML process, such as name screening or transaction monitoring, the risk-based approach is hindered by the sheer number of false positive alerts produced by inefficient technology systems. Investigating these takes time and resources, only for the majority of flagged transactions or customers to turn out to be low risk.

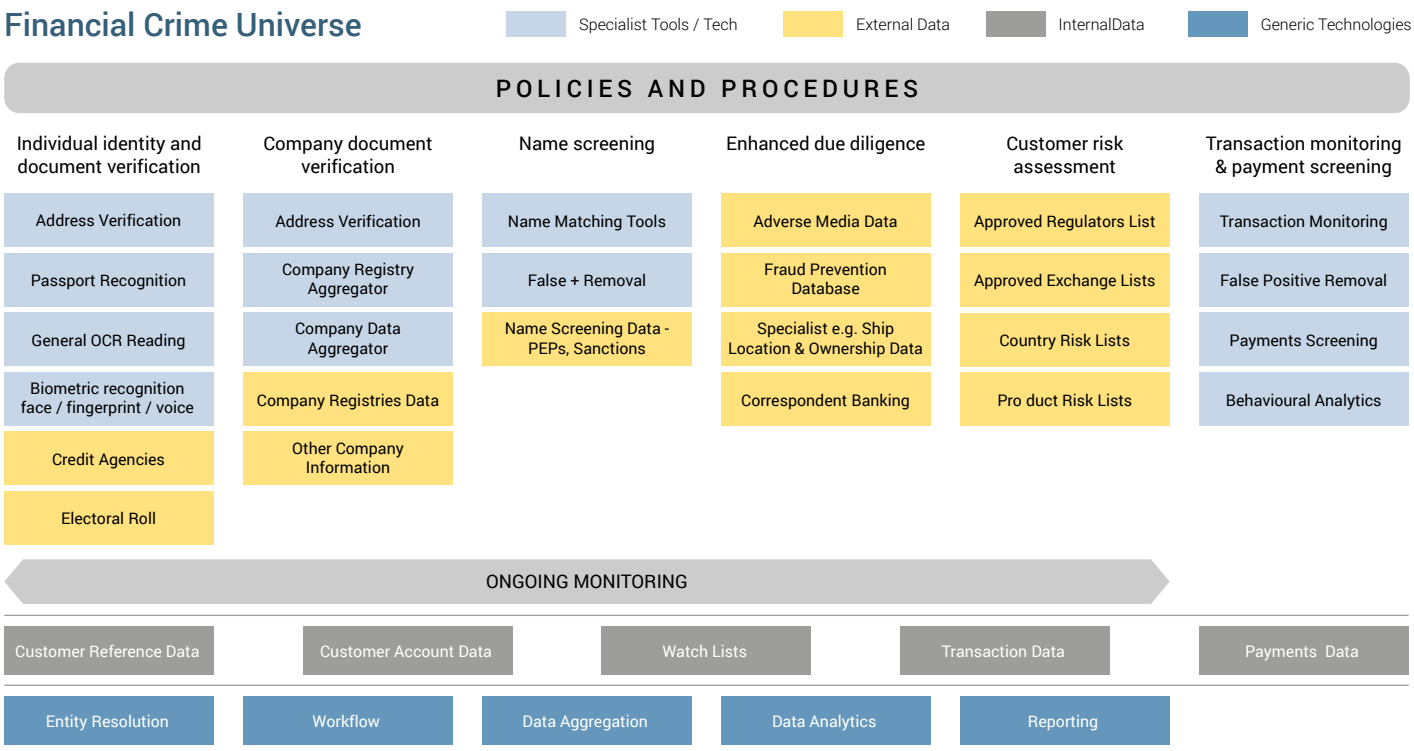
However, we should not put all the blame for these problems onto the financial institutions alone. External factors also have a part to play. Somewhat ironically, part of the issue is the ever-changing policy and regulatory framework for fighting financial crime, with the scope of the requirements growing each time there is a new set of regulations (see, for example, the broadening of the industries in the scope of the EU money laundering directives). In addition, global non-cash transaction volumes have grown significantly, up by 50% in 2017 from 2013, at 539 billion transactions per year. All of this makes the nut of financial crime compliance a very difficult one to crack.

VIEW FROM FSCom: A typical approach to managing AML in financial institutions

Anti-money laundering practices are, unfortunately, to their detriment, often extremely complex and not always easily maintained or carried out to the best practice, especially in the 'big banks'. Typically these banks were set up before the surge in stringent anti-money laundering policies and therefore, rather than factoring these practices seamlessly into their business plans many years ago, the policies along with the necessary teams and people responsible for the introduction and implementation of said practices can be muddled together in a confusing fashion. Larger organisations typically find it harder to adapt to new regulations for obvious reasons.

Banks with a huge number of employees do have the funding and therefore ability to create teams to specifically counter the various checks involved in AML. A fraud team, a transaction monitoring team, those focused on sanctions or jurisdictions. However, the technology and training utilized in each individual team can be different and lead to a lack of communication and the systems cannot work in sync together, as they really should to achieve best practice.

Some of the stories we read about in the press, or hear about on podcasts, are difficult to comprehend. The techniques used by Money Launderers can still be relatively simple, even lazy, and yet these criminals are getting away with it. Once revealed, the Danske Bank scandal seemed to throw up red flags everywhere, however, those huge sums of money were successfully laundered for 8 years between 2007 and 2015. This is obviously a very extreme case, though it outlines the necessity of teams and systems working together to catch the problem at an early stage.



We have created the Financial Crime Universe as a tool to explain just how complex financial crime compliance is within large financial institutions. From initial identification and verification through to ongoing transaction monitoring, managing anti-money laundering typically requires multiple internal and external data sources, several different technology systems, many separate teams often in different locations or lines of business and hundreds (if not thousands) of people with a range of skills and specialist expertise.

Even on a best endeavours basis, this fragmented approach to such a complex and all-encompassing set of requirements is unlikely to be successful, especially given the increasing pressure on costs and efficiency in the industry.

At the heart of the risk-based approach is being able to understand the risk that each customer - whether an individual or a company - poses to your firm. But this needs to be done dynamically, not just at a single point in time and to achieve this, it requires more than just an effective Know Your Customer process. The dots need to be joined across the whole customer lifecycle **and** between a customer and their transactional activity and behaviour.

Why should financial institutions act now?

Clearly, managing the risks of financial crime is not a new endeavour - but several separate forces are coalescing to create a critical need for more effective action.

1. Criminal sophistication and ever-changing typologies of financial crime

The techniques used by criminals to launder money and finance terrorism mutate and evolve, driven by increasingly sophisticated uses of technology and the ongoing digitisation of finance. Recently, criminals have been found to use on-line games as a mechanism for laundering money. There is a rise in the use of 'money mules' which are notoriously hard to detect and new methods such as 'cuckoo smurfing' continue to appear.

Unfortunately, crises such as the COVID-19 pandemic create new opportunities for criminals as explained by the Financial Action Task Force (FATF):

"The COVID-19 pandemic has generated various government responses, ranging from social assistance and tax relief initiatives, to enforced confinement measures and travel restrictions. While unintended, these measures may provide new opportunities for criminals and terrorists to generate and launder illicit proceeds."[4]

2. No let up in regulatory pressure and scrutiny of AML activities

In the USA, the UK and Europe, strong political mandates exist for improving the efficacy of anti-financial crime legislation. Published by the US Treasury early in 2020, the *National Strategy for Combating Terrorist and other Illicit Financing* aims to 'further the USA PATRIOT Act's purpose to "increase the strength of United States measures to prevent, detect, and prosecute international money laundering and the financing of terrorism".[5]

The *UK Government's Economic Crime Plan 2019-2022*[6] is an ambitious collection of policy, legislative and operational actions across both the private and public sectors, giving specific focus to enhance the supervision and engagement powers of the FCA and other AML supervisors such as HMRC.

Adoption of the EU's *Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorism Financing*[7] in May 2020 signals a further strengthening and harmonisation of the EU approach to AML and CTF.

Added to this political push is the continued level of regulatory scrutiny on financial institutions. Between 2015 and 1 June 2020, global regulators have issued $8,638m in fines for AML failings and this shows no let up. In the first half of 2020, a total of $706m[8] in fines has already been issued with some high profile cases such as the FCA fine of £37.8m imposed on Commerzbank.

3. Regulatory enforcement actions are focusing most on CDD and ongoing monitoring and AML Management

Failures in Customer Due Diligence/Monitoring and overall AML management are the most commonly cited issues in financial crime related enforcements globally. Data released earlier this year[9] shows that over the last five years, CDD failings have been noted in 115 enforcement notices and AML Management in 109 notices.

Both these activities are subject to fragmentation and siloed approaches and indeed, some of the more recent enforcement notices issued by regulators make this point. For example, the FCA's investigation into Commerzbank found that information about high risk clients was not being made available to transaction monitoring systems.[10]

4. Spending on financial crime compliance continues to rise when cost pressures are becoming more acute

Recently, LexisNexis found that the average annual financial crime compliance spend among mid-large financial institutions in Germany, France, Italy and the Netherlands ranges between $41.0m and $53.8m, with the UK at the higher end of that range[11]. Meanwhile, the banking sector in particular is experiencing significant cost pressures resulting from disruptive new entrants and Cost/Income ratios that are not improving in the long term.

Oliver Wyman suggests that to achieve a Return on Equity of 8% or over, European banks will need to cut costs by up to 15%[12]. However, gains from historic cost-efficiency measures appear to be shrinking, according to McKinsey, in their *2019 Global Banking Annual Review*[13], and they go on to indicate that 7 and 12% of operating costs are represented by KYC and AML compliance.

Squaring the circle between increased spend on fighting financial crime and the need to cut costs is therefore of paramount importance to the ongoing financial health of the financial services industry.

In summary, the risks of not acting are too high - firms must really begin to understand where they are now because fundamentally improving current AML capabilities is a must-have. Financial institutions need to start that journey now if they are to be prepared for current and future challenges.

PART 2: TOWARDS LEADING AML CAPABILITIES

What does a leading approach to AML look like?

We recently conducted a poll to find out what market participants' perceptions were of the term ' leading AML'.

Poll Question: What do you think of when talking about a leading approach to AML?

Combining fraud and AML	**11%**
Connecting transaction monitoring and KYC data	**28%**
Aligning transaction monitoring and trade surveillance for market abuse	**6%**
All of the above	**56%**

From these results, it is clear there is no single view of what a leading approach to AML should be. Clearly, without such a consensus, it makes it hard for firms to create a vision of what they should be aiming for to improve their capabilities. What is often overlooked, however, is that it is also critical for firms to understand where they are right now so they can plan their journey towards a leading AML approach.

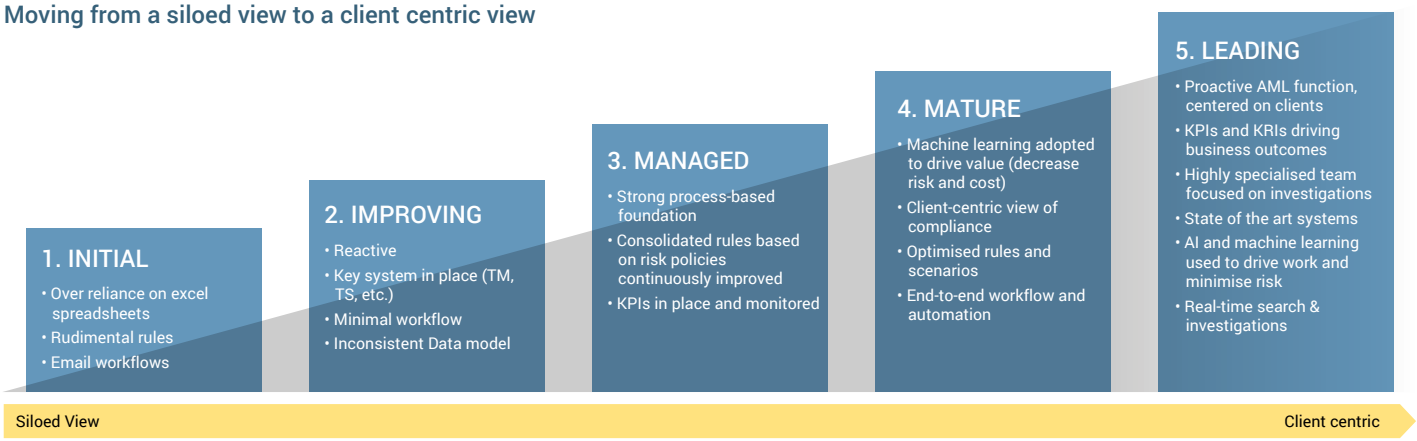
Given the diversity of the financial services industry in terms of company size, product offerings and geographical reach, firms are at very different levels of sophistication in their AML solutions and it can be hard for regulated institutions to know how they stack up against both their peers and best practice.

One of the most useful approaches we have seen to help firms benchmark where they are is a Maturity Model - *'a conceptual model that consists of a sequence of discrete maturity levels for a class of processes in one or more business domains, and represents an anticipated, desired or typical evolutionary path for these processes'*[14]. We have looked at several financial crime and AML-specific maturity models[15] but, like maturity models in other domains, we found them to be quite theoretical, without empirical foundations or not tried and tested in the relevant industry or lacking an insight as to how technology can support the move towards maturity. However, we have been working with London based compliance tech company Napier to understand the maturity model they have been developing for AML based on the experiences and situations of their customers - placing it squarely in the real world.

The Napier AML Maturity Model

This model has been designed to give regulated firms an understanding of the status of their AML and capabilities and the ability to continuously improve on the current state to achieve a more holistic and optimised state for combating financial crime.

Moving from a siloed view to a client centric view



There are five levels in the maturity model and as a firm progresses from the first to the last, AML compliance becomes more and more holistic and client-centric, culminating in a 'Leading' approach to AML which is:

- Proactive and centered around clients and customers
- Driving business outcomes through the use of KPIs and KRIs
- Comprising highly specialised teams focused on investigation
- Using state of the art systems
- Employing technologies such as AI and machine learning to drive work and minimise risk
- Conducting search and investigations in real time

AML capabilities are viewed through several organisational lenses in the model:

- **Strategy** - where do we want to get to as an organisation?
- **People and Culture** - how can we align our resources and culture to our strategy for AML?
- **Process** - how can we achieve operational excellence by streamlining and automating AML processes?
- **Data** - how can we get a high quality, single view of our data available in real-time?
- **Analytics** - how can we get the insights we need from our data for rapid and accurate decision-making?
- **Infrastructure** - what technology do we need to create a scalable and future-proof platform for AML?

Each of these lenses then has five dimensions, accompanied by detailed descriptions of where each dimension needs to be for each level of the maturity model.

High level overview of the Napier AML Maturity Model

DIMENSIONS	LENSES					
	Vision & strategy	**People & culture**	**Process**	**Data**	**Analytics**	**Infrastructure**
	Vision	Culture & leadership	Policies	Data quality	Data analysis	User interface
	Strategic planning	Functions & organisation	Procedures & workflow	Data modeling	Sandbox & impacts analysis	Accessibility (search)
	Governance	Team	Scenarios & rules	Data accessibility	Machine learning	Auditability
	Performance management	Roles	Alert management	External data (structured)	Dashboarding	Scalability
	Performance tracking	Knowledge sharing	Case management	External data (unstructured)	Reporting	Integration

For example, data is fundamental to the success of a firm's AML defences, but is also one of the biggest challenges that organisations face when transforming their systems and processes. Data quality, in particular, is an important factor to get right - and the maturity model shows how data quality improvements are made across the five stages of the model.

	INITIAL	IMPROVING	MANAGED	MATURE	LEADING
Data Quality	Multiple, inconsistent data repositories with poor customer and transaction data quality. High amount of spreadsheets	Multiple inconsistent data repositories holding information related to customers and transactions. No spreadsheets used for sensitive data	Standard data definitions, multiple systems holding different data, single version ofthe truth, data cleansed and standardised	Data lake consolidating all critical data in single repository; however data is difficult to traverse due to poor quality	Single data repository for transactions and customer, high quality information, ability to access all data in real-time. Big data fabric

In our view, Napier understands the needs of this market very well. Not only have they built a maturity model to benchmark the current AML capabilities, they have also built the technology to support it and to enable firms to move to the next level, wherever they are currently.

How to apply the AML Maturity Model to your business

We suggest a straightforward and logical approach consisting of three steps:

1. **Understand where you currently are by using the maturity model as a diagnostic tool**

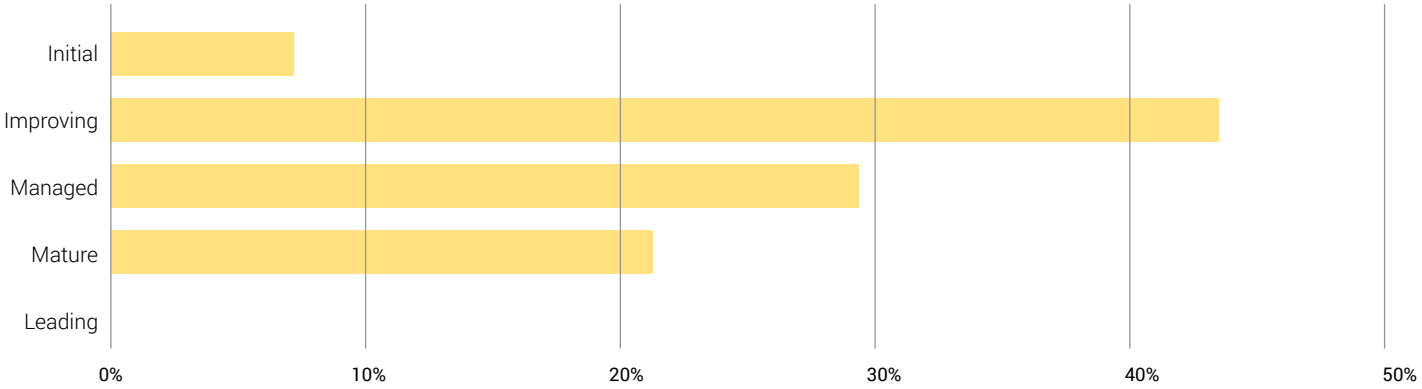
2. **Define your future targets across the short, medium and long term in line with your overall compliance and risk strategy**

3. **Identify what actions you need to take to reach these targets**

1. Understand the current state

A snap poll we took during an industry webinar revealed that none of the participants assessed their firms as being 'Leading' but there is clearly momentum towards maturity, with the majority of people identifying their firms as improving.

What do you think your organisation is on the journey to a leading AML approach?



For each of the six lenses, assess where your firm is across each of the dimensions by asking diagnostic questions such as:

- How is strategic planning performed for the AML function / capabilities?
- How do you track the performance of your AML capabilities?
- Do the various teams within AML perform similar functions or are they highly specialised?
- How is knowledge shared across all the people involved in AML?
- What degree of automation exists across AML processes and procedures?
- How accurate is your alert management process?
- How sophisticated are your controls around data access?
- How much use do you make of external sources of structured and unstructured data?
- To what degree do you use dashboards for analytics and reporting capabilities?
- Are you making use of statistical analysis / machine learning for analytics?
- How scalable are your current systems and infrastructure?
- How consistent is the user experience across the systems you use for AML?

You will end up with an idea of the level at which your organisation sits for each of these dimensions.

	INITIAL	IMPROVING	Managed	Mature	Leading
Strategy			●		
People & Culture		●			
Process			●		
Data			●		
Analytics		●			
Infrastructure		●			

2. Define targets - short, medium and long term

Next, you need to define a target state - in the example above, this firm may decide that it would like to achieve the 'Managed' level of the model across all the dimensions in 1 year. Breaking this down into measurable objectives might look something like:

- Remove duplication of alert management activities across all six lines of business
- Recruit a team of 5 data scientists to work on improving the use of data for better analytics and insights
- Reduce name screening and transaction monitoring false positives by 50%
- Create automated dashboards to replace manual spreadsheets used for senior management reporting

3. Identify what they need to do to reach these targets

The final step is to identify the concrete actions that need to be completed to move to the next level of the model and achieve these targets. A pragmatic approach is most likely to be successful - trying to change everything at once, whilst working within a budget and a low risk tolerance is unlikely to be the best course of action. We encourage firms to move towards a state of continuous improvement, rather than big-bang transformation programmes. This allows for a much more agile and scalable approach, as well as being able to take advantage of newer technologies that can integrate with your existing infrastructure.

VIEW FROM FSCom: Where should firms start?

The pressure here lies on the business to create a governance structure which is clear and coherent throughout. A key factor is confidence in the system, from all sides. The bank ultimately needs to feel confident when onboarding new clients that the systems they use to do this are reliable and thorough enough to safeguard against the inherent risks posed. The staff need to feel confident that they have been trained adequately to both spot any suspicious activity, but also that, once seen, they have a clear channel through which to take this information.

The big question is where does this all start for the clients? There is no straightforward answer to this, however taking a step back and having someone look at the organisation as a regulator or auditor would be a good place to start. Organisations, big or small, are beginning to understand that communication is key. A clear vision set out for all the people in the business to see and follow accordingly.

Methods to commit crimes in the financial institutions are becoming even more advanced and therefore the counter defence systems must improve as well. Going back to communication, this does not necessarily mean the technology used by banks needs to be more advanced, but rather the implementation of this technology needs to be more sophisticated.

How can innovative technology help?

In our view, whilst strategy, people and culture are clearly critical components of a Leading AML framework, the biggest advantages will be gained through the smart use of technology. User friendly, scalable technology products that enable a risk-based approach to AML and make the most of your data will ultimately lead to a more effective AML solution.
At RegTech Associates, we continuously scan the RegTech market and conduct deep research on vendors and products. Our database contains over 350 products which provide solutions for parts of the anti-money laundering problem, across a number of different disciplines:

- Identity and verification
- Customer on-boarding and KYC
- Name screening and Enhanced Due Diligence
- Transaction monitoring
- Financial Crime Risk Assessment

With so many products to choose from, it can be very hard for regulated firms to pin-point the one which will solve their specific problem or set of problems. We also understand how easy it can be for there to be a mismatch between customer expectations and product capabilities and how this can undermine trust in the relationship between vendors and regulated firms. But, to truly achieve holistic AML and move your firm to the next level of maturity, more advanced technologies such as artificial intelligence and machine learning are fundamental.

What should you be looking for in a solution?

First off, it is safe to say that there is not one perfect end-to-end solution that will move you straight to a Leading AML framework. The problem is just too big and too complex to allow for that. Instead, more and more we are seeing the adoption of best-in-class products that integrate together to give that complete coverage across all the AML capabilities. This means that product selection will vary significantly from firm to firm, based on where that organisation is on the maturity model but also based on the systems and infrastructure already in place.

Second, we agree with Napier's maturity model in that the use of artificial intelligence and machine learning is an essential part of a Leading AI solution, empowering analysts and identifying suspicious patterns in customer behaviour that may otherwise not be detected.

Here are our top considerations for selecting products to support your Leading AML solution.

1. Ability to solve your specific problem

All too often we see regulated firms select technology on the basis of either having existing agreements with a particular (usually incumbent) vendor or based on what their peers have chosen to use. In our view, this is a mistake - firms should hone in on the specific problem they are trying to solve and adopt a product based on that.

Do you need to aggregate several external data sources and automate the CDD process? A full customer lifecycle solution such as Fenergo or Pega Systems may not be the answer, but Encompass might be.

Is your rules-based transaction monitoring system too inflexible? Consider a system like Napier which can allow you to create, test and refine new rules in a sandbox environment as well as layering machine learning over the top to pick up the anomalies that are not detected by rules.

2. Optimised User Experience

Ideally, a Leading AML framework has a consistent user experience aross all systems, giving an integrated and holistic interface. Seek out products where UX is designed around specific types of user, based on their role - compliance, data scientist, manager - and even better, the processes that they have to perform.

3. Scalability

If we consider how transaction and customer volumes have grown in the last five years (as described above), this trend is very unlikely to be reversed. Add to this the business imperative for continued growth and the need for technology which is scalable at minimal cost is obvious. Demonstrating scalability can be difficult for vendors with less mature products but it can be advantageous to work with these tech firms as they are often more nimble and responsive than larger incumbent players. Do make sure you do your due diligence though - either through conducting proofs of concept or obtaining references from their other customers. clients.

4. Interoperability and integration

For a truly holistic and leading AML approach, you need seamless integration between systems, based on a single data repository with all users being able to access the data they need in real time. This is quite a radical shift from traditional IT architectures where interfaces between systems are batch-based. True integration can be achieved through the use of APIs which allow data sharing between different areas. Ideally, products you are selecting will have these advanced API capabilities so they can be simply ‘plugged in’ to your existing infrastructure which of course, must be similarly enabled.

AML and Machine Learning - Advanced Weapons for Fighting Financial Crime

ML is a type of artificial intelligence which uses advanced statistical models to parse huge data sets to identify patterns and make predictions. In the case of transaction monitoring, ML systems will use models to flag patterns of behaviour in transaction data that appear suspicious and do this in real-time.

Broadly, there are two types of ML models – supervised and unsupervised. Supervised ML models are 'trained' on large sets of historical data so they can recognise known patterns of behaviour that are likely to be suspicious, based on what has gone before. Unsupervised ML models are not trained – instead, they can identify patterns of behaviour without reference to existing typologies and are thus used to detect anomalies in data which are likely to be suspicious.

Machine learning (ML) has the capability to be more adaptive than rules-based systems and able to spot anomalous patterns in data that indicate something suspicious is going on, in real-time. Indeed, a recent joint report from the FCA and the Bank of England[15] has highlighted that anti-money laundering is a key use case for ML in financial services, and one where these firms see real benefits.

Generally in financial services, we are extremely good at detecting and understanding risks such as market and credit risk where there are huge sets of historical data that can be analysed statistically to help us predict risk in the future. This is analogous to supervised machine learning – historical data is used to train ML models to detect known outcomes. When it comes to financial crime, we can detect a proportion of suspicious transactions based on known money laundering typologies, but unfortunately, as we have seen above, new and unknown patterns continue to emerge.

For these Rumsfeldian unknown unknowns, we need to think more about financial crime in terms of uncertainty and less about risk. This is a distinction made by Knight as far back as 1921 and hinges on the idea that we are dealing with risk when, even if we do not know the outcome, we can measure the probabilities of different outcomes occurring. Uncertainty, however, means we do not have all (or any) of the information in order to set these probabilities in the first place. And this sounds very much like unsupervised machine learning – which can detect new and emerging financial crime typologies that have not been encountered before.

On this basis, we would expect that transaction monitoring systems based on unsupervised ML would be the most desirable solutions for financial institutions. However, there is an important trade off that has to be considered. Regulatory expectations (and good practice) around ML models require that the application of these models is transparent, and that the outcomes and decisions reached by ML systems can be explained. Unfortunately, levels of explainability decrease significantly when unsupervised ML models are used and firms must weigh up this balance between accuracy and explainability when implementing products using ML.

Winning hearts and minds

Finally, it is all very well setting out a neat and logical approach to achieving a leading AML approach, but we recognise that the real world is a lot more messy and challenging than a structured model. Overcoming some of these challenges will be critical to the industry's ability to improve the effectiveness of financial crime fighting.

Standing in the way is a complex combination of legacy technology, culture, resistance to the adoption of AI and machine learning, cost pressures and the sheer scale of the problem. We offer some practical solutions to these difficulties, gathered from our many conversations with both vendors and regulated institutions alike over the last few years.

Legacy technology is often cited as one of the biggest barriers to the adoption of RegTech, and whilst it is undoubtedly a hurdle, the solution does not have to be a complete 'rip and replace' to gain incremental advances. Instead, firms should look for tools that can augment existing capabilities - such as better data analytics, or secondary scoring systems for name screening or transaction monitoring. This approach is less risky and likely to be more palatable to regulators.

It has become something of a truism, but cultural change needs to be cascaded down from senior management. In the case of AML, it is imperative that Boards and senior executives view managing financial crime risks as a strategic objective rather than a box-ticking exercise for compliance. Leading AML frameworks that are client-centric will provide additional benefits - from reducing costs through to generating insights that can improve customer relationships.

Another issue that must be tackled at the most senior level is resistance to adopting artificial intelligence and machine learning. Education about this topic is crucial - not only to allay fears about people being replaced by machines but also to be clear about what AI can and can't do. Under the Senior Managers and Certification Regime (SMCR), it is clear that senior managers have a duty to understand both the advantages and limitations of the technology used in their part of the business and AI and ML are no exception to this. Finally, the scope and cost of implementing a leading approach to AML can be daunting. Despite it being the right thing to do, tackling this all at once can seem insurmountable. As the saying goes, the best way to eat an elephant is one bite at a time. Start small, with one business line or one customer segment. Take the time to create trusted partnerships with technology vendors, be clear and realistic about what the technology can achieve for you and show, rather than tell those holding the budgets, the art of the possible.

References

1. The United Nations Office on Drugs and Crime (UNODC) study to determine the magnitude of illicit funds generated by drug trafficking and organised crimes estimated that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered. In 1998, the IMF stated in 1998 that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's gross domestic product
2. https://www.europol.europa.eu/newsroom/news/does-crime-still-pay
3. McKinsey Transforming Approaches to AML and Financial Crime (September 2019)
4. FATF COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses (May 2020)
5. US Treasury National Strategy for Countering Terrorist and Other Illicit Financing (2020)
6. HM Treasury & Home Office Economic Crime Plan 2019 to 2022 (July 2019)
7. European Commission Action Plan for Comprehensive Union Policy on Preventing Money Laundering and Terrorism Financing (May 2020)
8. Duff and Phelps Seventh Annual Global Enforcement Review (August 2020)
9. Duff and Phelps Seventh Annual Global Enforcement Review (August 2020)
10. FCA Final Notice: Commerzbank AG (June 2020)
11. LexisNexis Risk Solutions True Cost of Financial Crime Compliance Study (March 2020)
12. Oliver Wyman European Banking 2020
13. McKinsey Global Banking Annual Review 2019
14. Becker, J., Knackstedt, R. & Pöppelbuß, J. Developing Maturity Models for IT Management. Journal of Business Information Systems (2009).
15. Accenture (2016) https://financeandriskblog.accenture.com/cyber-risk/finance-and-risk/the-stages-of-maturity-in-anti-money-laundering-aml-risk-assessment ACAMS (2012) https://www.acamstoday.org/the-need-for-improvement/O'Kane, T., Casserly, T., & McCartney, P. (2015). The financial industry maturity model for anti-money laundering. International Journal of Business Excellence, 8(4), 492-513. Gartner (2011) https://www.gartner.com/en/documents/1771015/gartner-s-aml-maturity-model
16. FCA and Bank of England Machine Learning in UK Financial Services (October 2019)

About RegTech Associates

Our mission is to bring all sides of the RegTech market closer together to realise the value of RegTech.

Founded in 2017, RegTech Associates is a privately held company based in London. Our experienced team has extensive industry and regulatory knowledge and we are often invited to speak at industry conferences and events.

We perform rigorous research, market scanning and analysis of the RegTech industry. This helps our technology clients better understand how they can grow, and our regulated firm clients discover who really solves their problems

For more information please contact info@rtassociates.co