We are now Refinitiv, formerly the Financial and Risk business of Thomson Reuters. We've set a bold course for the future – both ours and yours – and are introducing our new brand to the world.

As our brand migration will be gradual, you will see traces of our past through documentation, videos, and digital platforms.

Thank you for joining us on our brand journey.

REFINITIV™

SPECIAL REPORT: KYC AND AML POLICY

IMPLEMENTING BEST PRACTICE IN AN EVER-CHANGING REGULATORY ENVIRONMENT

THOMSON REUTERS™

INTRODUCTION

Heightened expectations from regulators have created an ever-more demanding regulatory environment for banks and financial institutions (FIs). Evidence of enforcement action is everywhere to be seen as firms are relentlessly held to account in the global battle against money laundering and other criminal activities. When setting internal policy, banks and FIs would do well to remember that a robust Know Your Customer (KYC) framework is still regarded as the most effective deterrent to financial crime.

In this special report on implementing an industry leading KYC and Anti-Money Laundering (AML) policy, we recap the key AML and KYC challenges faced by FIs and the best practice solutions to combat these, all shared in a recent Thomson Reuters webcast discussion, featuring industry experts from The Royal Bank of Scotland (RBS) and Thomson Reuters.

CONTENTS

KEY CHALLENGES SURROUNDING KYC AND AML

During a recent Thomson Reuters webcast, the panel of industry experts outlined the following key challenges for banks and other FIs, when attempting to draft a robust KYC and AML policy:

1. KYC policies are usually set by the compliance department or the AML financial crime advisory team, but the people responsible for implementing controls on a day to day basis are often not involved at an early stage. This can lead to a situation where a firm has a robust KYC policy, mapped to the right regulatory requirements, but it is effectively useless because it cannot be implemented. Moreover, policy-setting is often viewed as a once-off exercise, but the regulatory environment is constantly evolving, potentially leading to a disconnect between policy and regulation. Relevant staff members – from the head of KYC operations to the individual relationship managers – need to be engaged in drafting KYC policy and further, policies must be regularly reviewed so that they remain up to date.
2. Secondly, organizations that have a global footprint do not always take local nuances into account when developing global KYC procedures. This can result in a global KYC procedure that cannot be implemented in some countries. In order to bridge this gap firms need to ensure that all of the right people are around the table when KYC procedures are being drafted.
3. A third challenge is inconsistent or out of date source data that creates a knock-on effect with systems down the line. There needs to be a process to ensure that source system data is always kept current and is periodically cleaned.
4. Fourthly, where a customer is involved with different parts of the same organization and their details are entered on systems that do not talk to each other, records can become fragmented and may be duplicated. The right technology is needed to address this challenge and create a single view of each client across the organization.
5. Finally, seamless integration between the client onboarding system, the transaction processing systems and any other system that contains client files or where KYC information is recorded is critical. It is imperative that firms avoid a situation where, for example, KYC repository information is out of date, a customer has exited and one or more systems have not been updated as a result of the stale information.

PREPARING FOR A KYC AUDIT

The webcast panel then went on to discuss KYC audits and how when preparing for an audit, banks and FIs should be aware that the auditor(s) will be looking for the following:

- An up-to-date KYC policy and standards with evidence of senior management sign off.
- Evidence of organization-wide communication of all relevant KYC policies and procedures.
- Evidence of onboarding or refresh/remediation in accordance with current KYC standards.
- In the case of complex issues that require escalation, evidence and a complete audit trail documenting the decision that was made on the back of the escalation.
- Robust record-keeping and documentation that evidences that the firm is conducting KYC in an appropriate manner.
- Regular first line of defense quality assurance testing (within the business line that actually owns the client and the associated risk). This is becoming more and more important as there is a continual shift to the business owning the risk associated with a client.
- Where there is a detective process (e.g. sanction screening), evidence of any changes made to the customer profile as a result. This needs to include all alerts that were generated, an analysis of the alerts, the decision that was made on the back of the analysis and the resultant change to the customer profile.
- Training of all relevant staff, including training records and evidence of the escalation path and consequences for those not completing training.

THE IMPORTANCE OF TECHNOLOGY

Technology is the backbone of a successful policy, especially in an evolving KYC landscape. In a standard operating model regional teams generally follow a common process, but a lack of communication across regional hubs can leads to a host of problems - processes are often duplicated and multiple requests are made to the same entity via different routes, negatively impacting clients. Under this model, regional policies must be tied together to create consistency. Many FIs are, however, moving to an offshore model in an attempt to reduce costs – but this has implications for the IT infrastructure, because client services and core processes can be affected.

The IT landscape is generally an area of consistent underinvestment, with a pervasive 'just in time' mentality. What firms need to appreciate is that without a good IT infrastructure they will always be playing catch up. During the webcast, Lee Forsyth, Global KYC Client Consultancy Lead at Thomson Reuters commented, 'Several FIs on the wrong end of the regulatory radar have had to invest millions into IT to pull their models back together. This process involves revisiting all of their policies and procedures and trying to tie things together regionally. The net result of all of that is a remediation, which is painful, takes a lot of time and costs a huge amount of money.'

Ongoing transaction monitoring must tie back to the record that was built when a client was onboarded or when their record was last refreshed. This means that seamless system integration is crucial – an internally fragmented model with duplicate entities results in duplicate regions feeding into the same service. The backbone of good technology is a firm's API messaging capability and a key consideration when investing in technology is reducing operational risk as much as possible. Rather than implementing processes where individuals key information into systems, firms should opt for an automatic feed, with the ability to filter and control information. Regulatory responsibility lies squarely with the bank or FI and the regulator wants to see evidence that the right decisions have been made off the back of correct information.

KYC systems and technology must be flexible enough to enable key regulatory updates to be mapped in. To keep systems up to date, there should be a process to ensure that when regulations change, it is not only the policy that is updated, but all systems that could be affected.

Where there are reviews or quality assurance procedures being carried out, feedback loops should be implemented between KYC operations and the rest of the business. This ensures that all parties are aware of any adverse client information. Any alert that is identified within a KYC operation hub needs to be fed into the business so that the business can then take the proper decision. This could result in either exiting the client or a suspicious activity report, or transaction report being filed.

GETTING EXPERT HELP

Unsurprisingly, many banks and FIs are looking for expert help to manage this difficult environment. Forsyth elaborated, 'The industry is changing, what we are seeing is that there is a trend away from the service providers that do the remediations for you. Now we're trying to optimize the way that we deal with this business.'

Expert help may come in the form of a shared utility or a managed service. The shared utility model sees FIs participating in a service provided by a third party and paying only for the data they use. Information is collated from many different sources and made available through a single portal. FIs can use one or many of these types of utilities.

A managed service is slightly different and offers an end to end KYC solution. This involves using highly trained individuals who are constantly staying abreast of regulatory developments. Information needs to be readily available, and it needs to be current and accurate: the managed service model pulls together the key requirements of training, record building, monitoring and screening, and presents this information as one package.

WHAT DO FIRMS REALLY NEED FROM A MANAGED SERVICE?

Many onboarding, KYC and compliance teams spend a lot of wasted hours tracking and chasing documentation and evidencing reviews. This is the sort of heavy lifting that can be delivered by a managed service.

One of the vital things that a managed service needs to provide is the ability to track and monitor regulatory change as it happens across the globe. As Forsyth commented, 'Pulling all the relevant information together before those regulations bite is crucially important.'

Transparency is also key. Banks and FIs must be able to demonstrate that they know their clients and must be able to provide step by step evidence that they have built robust files and collated information.

A managed service provider needs to be able to provide accurate, clear, succinct information – and quickly. Many firms have a refresh process that covers one to five years at a time, depending on the risk profile of their clients. But records become stale very quickly, so using a proactive tracking model that monitors information from the primary source is crucial. Based on Thomson Reuters research (see figure 1), during a nine month period and with a population of approximately five thousand records, the following changes can be expected:

30% - changes to directors and controllers

20% - changes in beneficial ownership or control

17% - changes in address/location

10% - name changes

5% - changes to regulatory status

3% - changes to listing status

3% - mergers

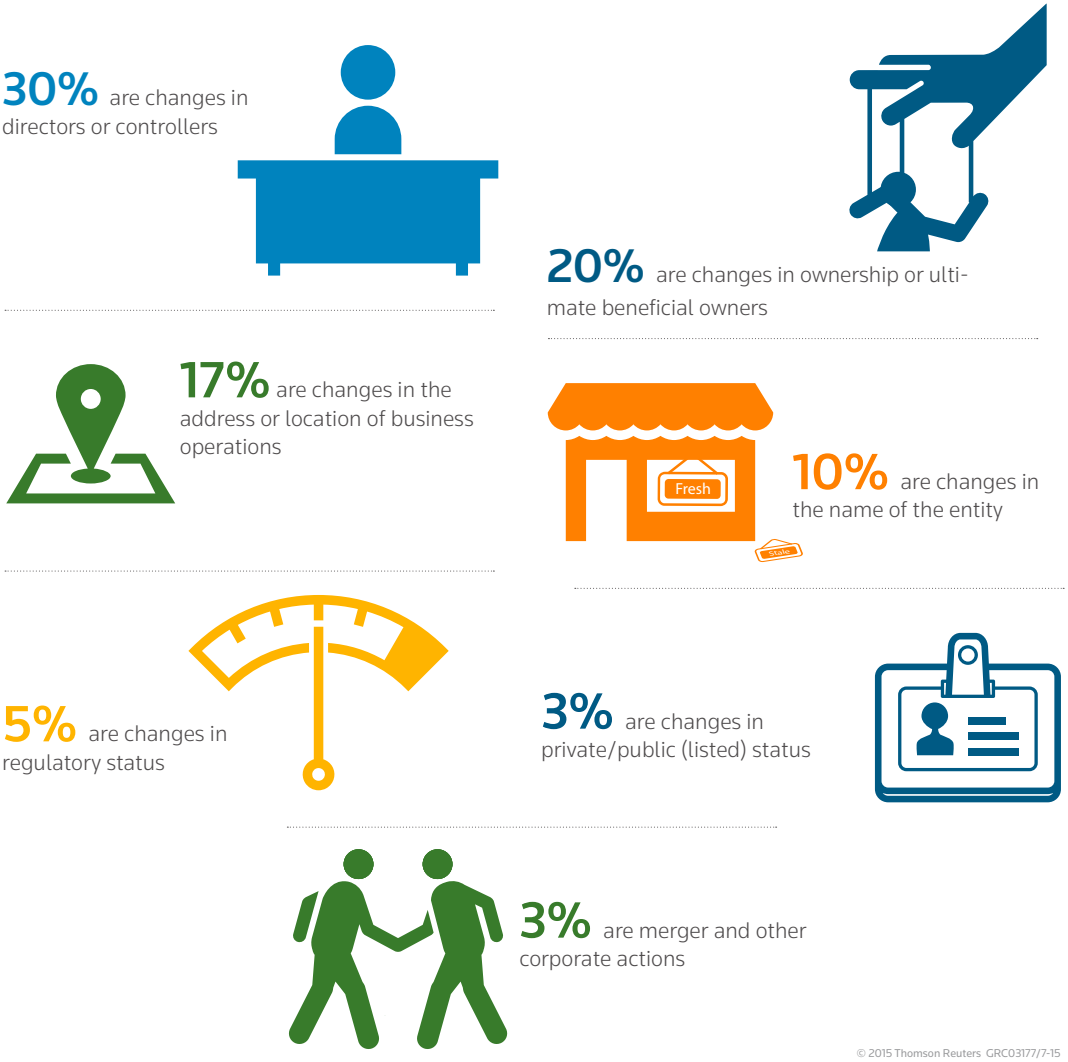

FIG 1: IDENTITY MONITORING - COMMON CLIENT IDENTITY CHANGES

Regulatory bodies monitoring FIs are quite rightly expecting them to monitor these changes and it is vital to appreciate that your risk profile can change very quickly.

CHECKLIST: QUESTIONS TO ASK YOUR PROVIDER

When selecting a managed service provider, run through these critical questions and make sure that these capabilities are in place:

- Can you verify a client's identity through collection and validation to a common market-leading standard?
- Can you screen clients and all their associated parties against all key lists?
- Can you search against adverse information and adverse media?
- Can you identify all ultimate beneficial owners and senior management officials?
- Can you publish records with clear risk rankings and red flags? (This is key information that analysts and consultants need to make informed decisions.)
- Can you automatically rescreen clients and related parties if needed?
- Can you monitor the identity and the status on a daily basis?
- Can all this information be shared in a highly secure portal?
- Does the system integrate? Do you have API capabilities? Can this information be fed, pulled or pushed?
- Do you have the capability to track regulatory change globally?

CONCLUSION

Global regulators will continue to demand ever-more rigorous KYC and AML controls from banks and FIs. In order to stay ahead of the regulatory curve, it is crucial that firms implement best practice and appreciate the vital importance of the right technology. Furthermore, using a trusted external partner to optimize KYC policy and remove some of the 'heavy lifting' is a solution that is growing in popularity because, as Forsyth concluded, 'When you optimize your KYC, it frees you to focus on business critical core functions such as expanding your footprint, strengthening your client relationships and establishing your enterprise as best in class.'

RISK MANAGEMENT SOLUTIONS FROM THOMSON REUTERS

Risk Management Solutions bring together trusted regulatory, customer and pricing data, intuitive software and expert insight and services – an unrivaled combination in the industry that empowers professionals and enterprises to confidently anticipate and act on risks – and make smarter decisions that accelerate business performance.

For more information, visit risk.thomsonreuters.com

THOMSON REUTERS™