A brave new year: Ensure your KYC compliance in 2017 and beyond

By Malcolm Wright, Global Head of AML and Fraud Proposition, Thomson Reuters

If 2016 was a year of political upheaval, 2017 looks set to be similarly disruptive for anti-money laundering (AML) and countering the financing of terrorism (CFT) compliance. Both know your customer (KYC) and secure your customer (SYC) will play a significant part in shaping the regulatory landscape. Here is a snapshot of major themes and trends we see happening this year and beyond:

**Regulation, regulation, regulation**

In 2008, the world’s regulators issued approximately 24 alerts per day. In 2015, this number exceeded 200,¹ providing hard evidence that as criminal and corrupt behavior adapts, so regulation has grown exponentially to keep up.

2017 brings a new raft of significant measures, many of which will have far-reaching effects beyond the borders of the issuing countries and regions. Kicking the year off was the New York State Department of Financial Services’ (DFS) final rule for transaction monitoring and filtering, which came into effect on 1 January.² Later this year, we will see the EU 4th Anti-money Laundering Directive³ come into force, together with an in-progress amendment touted as the 5th Anti-money Laundering Directive.⁴ The EU Funds Transfer Regulation,⁵ and the revised Payment Services Directive (PSD2)⁶ will also come into effect.

At a national level, regulation and regulatory oversight is also facing an overhaul. In the UK for example, the Financial Conduct Authority’s Senior Managers Regime (SMR)⁷ extends further to the Certification Regime. Meanwhile the Criminal Finances Bill,⁸ which aims to be law by March, will introduce a strict liability crime for failing to prevent tax evasion and a possible new amendment introducing a failure to prevent economic crime, a wider scope that would cover AML and fraud. Importantly, these changes extend their reach beyond the borders of the UK, thus organizations outside the country should be aware.

Mention should, of course, also be made of the EU General Data Protection Regulation (GDPR).⁹ Read more on this under “Secure Your Customer.”

**Culture, culture, culture**

The message from regulators is clear; the days of tick-box compliance are over. Indeed, with such a tidal wave of regulatory change heading towards the shores of compliance professionals, it requires a step-change to ensure the challenge can be met. And this will require the participation of the entire organization rather than the chosen few in compliance.

Culture starts from the top with leadership engagement and works down through the organization with a properly controlled risk environment and appropriate, regular training for employees. In this last respect, compliance professionals should take note that an inadequately trained member of staff, even if he or she is not front-line compliance, may put the organization and MLRO at financial, reputational and regulatory risk.

**Review your “RegTech”**

Technology may not yet hold the key to fully automated, low-cost compliance, but investment in the right RegTech tools can ensure that exposure to AML/CFT and other risks is minimized or mitigated, and that compliance costs can be appropriately planned and managed.

Nascent technologies such as blockchain and artificial intelligence offer promise, but it is still too early to reliably call on them in the compliance arena. In the meantime, ensuring KYC screening¹⁰ system settings and transaction monitoring¹¹ rules have been reviewed and optimally adjusted, and indeed that they are being used correctly by compliance staff, can increase the reliability and quality of the compliance effort.
Secure Your Customer (SYC)
Returning to the previously mentioned GDPR, there is now an acute focus on protecting your customers’ data, or SYC. Perhaps the three key takeaways from the legislation in this respect are:

• Breaches must be reported within 72 hours
• Systems must encompass “security by design”
• Organizations should ensure all of their systems are adequately protected and monitored with evidence to this effect – including KYC and transaction monitoring compliance systems

There have been numerous reports that 2017 will be the “year of cyber security,” and regulators will be taking a keen view to ensuring that organizations adhere to the principles of good data governance throughout their operations.

Now it’s personal
A further key theme this year – and one ignored at your own risk – is personal liability. Each individual compliance professional must take ownership for his or her actions and fully assess his or her own personal regulatory risk management strategy to ensure compliance and avoid liability. Recent enforcement action, such as the 2016 groundbreaking decision by a U.S. federal district court in Minnesota that compliance officers at companies subject to the Bank Secrecy Act (BSA) can be held personally responsible for AML failures, has illustrated that regulators will not hesitate to impose the full force of the law and hold individuals to account. The message is clear: Personal liability is here to stay.

Make your voice heard
With new regulation often comes consultation. Indeed, both the UK and Australian governments have issued several consultations in the past few months that have specific interest to compliance professionals. Such consultations can and do shape policy, and regular engagement in this way or directly with regulators, can help ensure that legislation is clear, effective and not unduly onerous.

Partner up
Finally, going it alone is very often not sufficient in this complex and rapidly evolving world of compliance regulations. Risk, compliance and internal audit functions should therefore include outsourcing in all their monitoring plans and consider engaging managed services from an external provider. KYC, enhanced due diligence and screening managed services offer a raft of benefits, including:

• Reducing the pressure on often over-stretched internal compliance departments
• Lowering ongoing compliance costs
• Speeding up turnaround times, both when onboarding new clients and when refreshing client records
• Providing superior data privacy and protection
• And much more

Author’s bio:
Malcolm Wright is the head of AML and Transaction Monitoring for Thomson Reuters Customer & Third Party Risk where he leads Thomson Reuters AML, CFT, and fraud transaction monitoring propositions. Customer & Third Party Risk is one of the fastest growing sectors in the Thomson Reuters Risk segment, and Wright has been an essential benchmark within this segment ever since he joined in 2012. Redefining the current product offerings under his remit into a market-winning business strategy, he has ensured continuous improvement in productivity, revenue, efficiency and customer satisfaction.

Visit risk.tr.com

1 Thomson Reuters Regulatory Intelligence
2 NYDFS Final Rule on Transaction Monitoring and Filtering (Part 504)
7 UK FCA Senior Managers Regime
8 UK Criminal Finances Bill
10 Thomson Reuters World-Check One
11 Thomson Reuters Transaction Monitoring
12 U.S. District Court Denies Motion to Dismiss FinCEN Complaint Against Former Chief Compliance Officer of MoneyGram