Analytics-powered tools have been widely adopted across different industries for different purposes as the world becomes ever-more connected and businesses work towards the most recent Holy Grail: digital transformation. However, compliance teams have demonstrated some reluctance when it comes to hopping on the technology bandwagon. At the end of 2016, only a handful of banks around the world were working with advanced analytics and artificial intelligence (AI) technology to improve their risk and compliance efforts.

“The compliance teams are responsible for preserving the integrity and reputation of that organisation, which can be severely damaged should they inadvertently allow criminals to use their services to fund illicit activities,” Frank Holzenthal, FICO

Compliance teams, especially in financial services organisations, are under more and more pressure from ever-tightening national and international regulations. Acting like an internal police force that ensures its organisation is compliant with applicable laws and regulations, compliance teams are responsible for preserving the integrity and reputation of that organisation, which can be severely damaged should they inadvertently allow criminals to use their services to fund illicit activities. Solutions in areas such as ‘know your customer’ (KYC) and anti-money laundering (AML) help risk and compliance teams stay on top of all transactions for this purpose.

As the world plunges into an era of high uncertainty, the upcoming years will see financial services organisations adopt and deploy best-in-class analytics-powered tools as part of their efforts to remain fully compliant and to fight financial crime and terrorism.

With that in mind, here are the top five trends that will power the analytics-in-compliance revolution.

Analytics to isolate terrorism funding

Last year, we saw the number of terrorist attacks across Europe and the Middle East rise again. After the events in Belgium, France and Turkey – to name just a few – there has been increased focus on the urgent need to thwart all flows of funds to terrorist organisations. Bank bombings, such as those we saw in Iraq in January last year, are one way to eliminate ISIS funds, but financial institutions need to take the fight off the ground to truly cut off terrorist groups at the source of their illicit income.

Hiding and laundering money without being detected will be a mission-critical function for terrorists worldwide and financial institutions will have to ensure that they are doing everything in their power to stop them. Failing to do so will be highly detrimental – no one wants to be the one who let the bad guys get away.

“One of the challenges investigators face is migration. The movement of people from one place to another adds a layer of uncertainty that investigators need to take into account in their AML and anti-terrorism efforts”

One European offshoot of a North African bank group experienced this first hand just before the terrible Paris attack in November 2015.1 One of the IS terrorists involved attempted to transfer money to another well-known terrorist, also involved in the attacks. The Paris branch of this bank used recently updated analytics-powered AML technology and was able to properly block this SWIFT transaction. Unfortunately, the customer in Paris – the terrorist – complained to the North African headquarters about the cancelled transfer. The headquarters did not use advanced analytics for their KYC or AML programmes and therefore the screening process failed to detect that the customer was a match with the sanction lists. The transaction was authorised and the terrorist got the money he needed.
The bank is still under investigation following this incident and its reputation has been severely damaged. As part of the effort to prevent this sort of error from happening again, the bank has now deployed powerful analytics-powered AML technology across all branches, including the North African headquarters.

This is a powerful cautionary tale about why we need analytics and AI to help us to maintain strictly legal banking. Corporate reputational risks are too high for any organisation to fail to take proper action, so we expect to see significant investments in technology to ensure KYC and AML programs are best-in-class.

Illicit migration

Financial crime and AML efforts face challenges that can only be solved by widespread adoption of the best analytics available, combined with continuous research and development of new models to integrate into KYC and AML tools. One of the challenges investigators face is migration. The movement of people from one place to another adds a layer of uncertainty that investigators need to take into account in their AML and anti-terrorism efforts.

Kumar C. Kibble, Homeland Security Investigations regional attaché to the Netherlands for the US Department of Homeland Security, reported on ‘New Challenges in Illicit Migration’, a problem that is being aggravated by the Eurozone’s troubles and Brexit. Kibble foresees that criminal networks will continue to exploit the high demand for facilitation services and that small smuggling networks will gradually be taken over by larger criminal networks. This new migration challenge further complicates the efforts to fight financial crime and money laundering.

Increasing turmoil in different parts of the Middle East, as well as tensions in former Soviet Union territories, are causing illegal migration to spike. Just like terrorism, illicit migration and human trafficking activities require funding. For these operations to work, large networks of collaborators are put in place and developed across several countries. These networks also need to be maintained over time, which is not cheap.

The only way to truly stop these activities is to cut off their funds. This means that financial crime investigations have to monitor money flowing in and out of countries receiving migrants in addition to all other movements and behaviours they already cover. Without the right tools and technology, monitoring all transactions around the world and detecting those that are funding illicit activities would be a Herculean task for any team. It would be impossible to keep track of them all and even harder to investigate them to detect illegal activities.

"KYC will screen sanction lists to ensure that no bank onboards a customer who’s on a black list and that they are never able to transfer money to anyone they shouldn’t”

It is not only illegitimate migration that poses a challenge to investigators. Legitimate migration can sometimes make it harder for compliance teams to determine if an activity is fraudulent or not. Visiting or moving to a new country can create anomalies in your behaviour that AML and KYC systems can read as high-risk. Most KYC and AML solutions work with behavioural analytics to some extent to help ascertain behaviour that is risky as opposed to simply unusual.

Generally, KYC will screen sanction lists to ensure that no bank onboards a customer who’s on a black list and that they are never able to transfer money to anyone they shouldn’t. At the same time, AML solutions can all customer behaviours for anomalies. Each customer is allocated a profile based on a series of characteristics and their behaviour is continuously checked against ‘normal’ behaviour for the person – based on historical data – but also against ‘normal’ behaviour for their peers. Thanks to smart, self-learning analytics, the systems constantly absorb information from all transactions and adapt over time, evolving as customers’ circumstances change.

When a person travels or migrates without alerting their bank and then transfers money to and from a new country, that is a new behaviour that the KYC and AML models haven’t seen before for this person. This change in behaviour that can’t be explained – and that is not similar to that of the peer group – will be picked up by KYC and AML programmes and flagged to the risk teams as a suspicious activity, even though it isn’t.

Last year, for example, a German savings bank detected a suspiciously high volume of money transfers through Luxembourg. On investigation, it turned out that refugees arriving in Germany discovered that they could legally apply for a credit card in Luxembourg for free. This kind of unusual behaviour can easily be mistaken for money laundering. Only through constant technological innovation and development can KYC and AML solutions be refined to the point where legal migration is no longer a challenge.

Off-shore no more

Data leaks have commanded international headlines throughout the last few years. Companies in all industries have seen confidential information compromised in one way or another. In April 2016, 11.5 million files and 2.6TB of information from the database of the world’s fourth-biggest offshore law firm, Mossack Fonseca, were leaked.2

This ‘Panama Papers’ leak was unprecedented and it put tax avoidance in the spotlight. The documents exposed hundreds of wealthy people, including 143 politicians, who had been using tax havens. This raised global concerns about money laundering and financial crime because, while most off-shore money movements are legal, many crooks take advantage of anonymous company structures to finance illicit activities. It became
دریافت فوری متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات