AML Predictions–What Lies Ahead for the Compliance Industry in 2023?

Byline: Adam McLaughlin, **Global Head of Financial Crime Strategy & Marketing, AML**

A Quick Look Back on 2022

2022 was a year of change that took the financial crime and compliance industry on a roller coaster ride. The U.K. pushed through the Economic Crime Act at lightspeed, and the sanctions landscape changed overnight with the Ukraine and Russia conflict. There was political uncertainty both in the U.K, with the constant Prime Minister changes, and in the U.S. thanks to midterm elections. Potential leadership changes could have significantly impacted the focus and direction of financial crime. But safe to say, we made it to the end of this tumultuous year with our strategic direction intact.

Globally, organizations have been talking about entity-centric financial crime, or end-to-end customer life cycle risk management, as the key to AML effectiveness. Effective risk management requires a different approach to understanding customers. At the heart of this approach is integration. Data, systems, and teams must be integrated to provide a holistic view of each customer. A risk-based approach, as sought by many regulators, industry experts, and organizations, needs to be based on this comprehensive understanding of customer risk to be effective.

Enterprise risk management also took center stage this year, since one of the biggest risks that organizations face is the risk exposure of their customers. In this area, entity centric, and the various iterations of the entity-centric approach, has become an increasingly important strategy as the regulated sector looks to understand risk across the organization.

I'm predicting an interesting 2023 with increased attention on evolving threats, more targeted focus on the most socially and environmentally destructive financial crime threats and heightened regulatory focus. Read on for my top 5 AML predictions for 2023.

Prediction 1: The Battle of Privacy versus Information Sharing

Criminals don’t rely on one financial institution for all their financial needs, they diversify across multiple institutions and multiple jurisdictions within those institutions. They use corporate vehicles, namely because they provide the anonymity that criminals crave. As such, transparency and information sharing across the sector are critical to identifying criminal networks and activity.

Globally, regulatory bodies and government institutions have made efforts to take away the corporate veil of secrecy by introducing laws which require greater transparency of corporate controllers and Ultimate Beneficial Owners (UBOs). The AML Act in the U.S. is due to introduce UBO registers, and the recent Economic Crime Act in the U.K. introduced legislation requiring overseas corporate entities owning U.K. property to disclose the property’s UBOs.

The 5th Money Laundering Directive in the EU introduced the requirement for open, freely accessible public UBO corporate registers across all members states. But this has, unfortunately, had the brakes applied: A recent European Court of Justice ruling said that the requirement of the 5th Money Laundering Directive for open public registers of UBOs is invalid and an affront to the right to privacy of the UBOs of companies. Since this ruling, several EU jurisdictions have restricted public access to their corporate registries. This case is a powerful example of the battle between privacy and transparency in the fight against financial crime.

In some respects, this ruling takes us back years. Because if more people can access the data, then we’re more likely to join the dots. However, there’s a silver lining. The court did accept that certain sectors, such as the press, are instrumental in helping to fight financial crime. These sectors and organizations should be entitled to access the registers.

This battle of privacy versus information sharing is also being played out in private-to-private information sharing initiatives. Within the industry, there’s a growing desire to share information on suspicious activities, criminal entities, and individuals. Many initiatives have been established for KYC and transaction monitoring to aid information sharing and monitor collectively.

Those initiatives encounter one hurdle: privacy. Until the matter of protecting Personally Identifiable Information (PII) is resolved, or there is a clear legal gateway to share information, then true information-sharing initiatives will falter before they gain any traction.

I predict that this conflict will be a central focus for many in 2023, especially now given the European court ruling on public corporate registries. The question is which will win out: Will we get greater freedom to share information and increased transparency, or will the right to a private life and privacy overrule the desire of the financial crime community?

Prediction 2: Focus on The Real Threats

2023 will be the year when the industry targets their efforts on monitoring and detecting real financial crime threats instead of generic monitoring, which today requires significant effort even when monitoring low-risk activity.

It’s no secret that high false positive rates plague many organizations. What may be surprising is that many organizations put significant resources and effort into monitoring the wrong areas of their business—what is ultimately low-risk activity. This stems from historical regulatory guidance, notifications, and findings that encourage financial institutions to monitor these areas of the business more intensively than risk assessments deem necessary.

Most organizations focus on the financial crime risks of their retail and domestic customers. However, often no one individual retail account presents a significant financial crime risk. In fact, most of the risk lies in other areas, including capital markets, international trade, and corporate or commercial banking. These areas attract money laundering activity because it’s easier to move vast sums of money under the guise of legitimate income.

That’s not to say retail banking is riskless, but instead, that risk centers on very specific use cases. For example, mule accounts or human trafficking activity where victims are usually forced to open accounts in their own names, but the accounts are controlled by the trafficker. Historically, detection scenarios have been too generic to identify these specific types of activity.

It has already started, but in 2023, we will see greater focus on monitoring and detection of truly high-risk activity. The first will be greater attention on the high-risk verticals such as corporate banking (including trade finance and capital markets.) These verticals have been in focus for a while. In fact, the capital markets vertical has been front and center for many years since the Deutsche Bank mirror trading typology and the thematic review released by the FCA in 2019. In 2023, organizations will actively seek new technology solutions to overcome existing challenges in detecting suspicious activity in these verticals.

From a predicate crime perspective, there is growing demand to accurately identify high-impact predicate crimes. There is already a pretty good understanding of the modus operandi of these crimes, but in 2023 we will continue to improve our understanding of these crimes. Organizations will increasingly have the right tools to allow them to map these typologies in their monitoring solutions. This will enable them to accurately detect when an individual is potentially a victim or suspect involved in human trafficking. It can also help to identify when individuals or entities are involved in wildlife trafficking.

This change in focus in 2023 will bring greater effectiveness in how we target and mitigate illicit activity, ensuring organizations can assign the right resources to the threats that have great impact and pose the most financial crime risk.

Prediction 3: Continued Focus on DNFBPs

Designated Non-Financial Businesses and Professions (DNFBPs) such as art dealers, estate agents, notaries, lawyers, company service providers, accountants, and casinos, are businesses that pose a money laundering risk but are not classified as financial institutions. These businesses pose a risk because they are gatekeepers to the financial sector. Through DNFBPs, individuals and corporates can place vast sums of money and assets into the financial system.

Most of these businesses have direct relationships with their customers, more so than banks. These businesses place their customers' money into banks (often in the name of the DNFBP business) and in some cases, have more intimate knowledge of the customer's history, behavior, and source of wealth, especially for higher net worth individuals. They might have regular face-to-face meetings with customers, and help them with day-to-day activities, such as dealing with assets, businesses, tax affairs, and legal matters. If anyone is going to understand if an individual is legitimate or not, it will be these businesses. Consequently, most DNFBPs are in a better position to more accurately spot suspicious activity compared to banks, especially if all that banks see is the financial movements of the DNFBP business account and not the underlying individual or business these activities relate to.

A large number of countries have introduced regulations to regulate DNFBPs, such as the money laundering regulations in the U.K. However, each industry is often supervised by its own regulatory body, such as the Solicitors Regulation Authority or the Chartered Institute of Management Accountants. This introduces risk due to inconsistent application, enforcement, and oversight of the regulations. How can we ensure compliance with regulations and start to fight money laundering in this sector if different bodies regulate different businesses (if these businesses are even required to report suspicious activity in the first place)?

On the other hand, some countries like Australia and the U.S. do not regulate all DNFBPs. In fact, recently the U.S. senate blocked the Enablers Act, which would have required many DNFBPs to conduct AML checks on their customers.

FATF clearly states in their 40 recommendations that DNFBPs should conform and comply with AML regulations and best practices. Recommendations 11, 12, 15 and 17 to 21 apply to DNFBPs with a specific section for DNFBPs in recommendations 22 and 23. There continues to be much focus on DNFBPs. They're in the regulatory spotlight and high priority for financial crime professionals. To win the fight against financial crime, we all need to work together to identify, detect, and report suspicious activity. We cannot do this without the support and co-operation of DNFBPs.

I believe in 2023 there will be increased pressure to align regulations globally for DNFBPs. A strengthening of enforcement will also result in larger fines and put greater pressure on those DNFBPs that fail to comply or facilitate illicit activity through their businesses.

Prediction 4: Collective Risk Management

Enterprise Risk will be the term of the year in 2023, especially in the context of understanding customer risk. Risk is not static or siloed. It's not exclusive to AML, either. There are several risk factors that can impact how risky a customer is. Those factors ultimately help financial institutions understand the potential financial crime risk of a customer. These risk factors include AML risk factors, like transactional, KYC and screening risks, but also fraud risk, credit risk and, of mounting importance, Environmental, Social, and Governance (ESG) risk. These risks should not sit independently—if we're assessing customer risk, all these factors need to be considered to understand the collective risk of each customer.

Traditional enterprise risk goes beyond assessing customer risk. It's wider still, considering aspects such as liquidity risk, operational risk, strategic risk, financial risk, and hazard risk to name a few. In 2023, an enterprise risk approach will be taken to understand customer risk much more granularly than what is achieved today.

All customers are dynamic. Over time, their behavior, financials, and transaction types will change, even more so with corporate customers. Some customers will invariably be criminal or turn to crime during the tenure of their relationship with an institution. Other customers may become victims of crime, including fraud.

These aspects of risk are important indicators of how financial institutions should interact with the customer. However, inside financial institutions, these risk indicators are discrete, stored on separate systems and accessed by disparate teams. This results in a disjointed, inaccurate enterprise-wide assessment of the customer and their risk.

Regulators and bodies such as FATF call for organizations to adopt a risk-based approach to managing risk, but this cannot be done with disjointed systems, data, or teams. This is why I believe the next evolution of the risk-based approach will be to connect these disparate data sets and systems to understand, contextually, the risk of each customer. Combining their credit, ESG, AML, and fraud risks to achieve an overarching risk score, or trust score, for the customer offers a holistic risk picture that helps to fuel better monitoring and detection. It also allows for more accurate revenue decisions based on how trustworthy the customer is. This evolution will gain traction in 2023.

The convergence of fraud and AML (FRAML) is another trend that falls closely in line with the evolution to enterprise-wide customer risk evaluation. Globally, there is an increasing number of financial institutions actively looking to converge their fraud and AML functions and systems. The reason for this convergence? It’s for better risk management and assessment of both customers and transactions. This FRAML trend confirms there’s traction in industry to move toward an enterprise view of customer risk.

Prediction 5: ESG Risk Becomes a Financial Crime Issue

This last prediction ties in well with prediction #4 about enterprise risk. In 2023, ESG will find its way into the realms of financial crime. What does ESG have to do with financial crime? ESG is not just about ensuring a business has green credentials and is operating in a carbon neutral way. Nor is it just about looking at stakeholders and if the company is acting inclusively and paying fair wages. It's also about whether the business is having an adverse impact environmentally or socially, which could include anything from illegal logging or fishing to employing slave or child labor.

These are all ESG issues and can be committed by a:

- Direct customer of the financial institution
- Sub-contractor
- Third party somewhere along the supply chain

These matters are all crimes. Any proceeds generated thereafter would amount to proceeds of crime and could implicate the direct customer of a financial institution. Therefore, it's critical that all financial institutions consider their ESG risk when it comes to monitoring and investigating financial crime.

For example, take illegal fishing. This crime is responsible for the destruction of marine ecosystems and loss of revenues for local fishermen, yet provides criminals up to USD 23 billion in revenues annually. It's a classic supply chain issue. Financial institutions need to know who their customers are, the nature of their customers, and now, who their customers deal with. Failing to do so could result in the financial institution unwittingly banking a customer engaged in illegal fishing activity and, ultimately, dealing with criminally derived funds. With ESG risk data, institutions can identify risky connections earlier and mitigate associated risks. In this illegal fishing example, with ESG risk data present, the bank would be better placed to understand the risk of involved entities, exit unmanageable customer relationships, and mitigate the risk of facilitating money laundering.

Illegal fishing is just one example of where a predicate crime can be committed by seemingly legitimate companies. Furniture companies, food manufacturers and agricultural customers could be directly or indirectly engaged in ecological destruction such as illegal deforestation. Jewellers and mining companies could be directly or indirectly engaged in illegal mining or the use of slave or child labour. Logistics and shipping customers could be engaged in the transport of illicit goods, including products from illegal wildlife trade. Do you know your customers well enough and monitor their transactions sufficiently to identify this type of activity or connection?

There is another area where ESG and financial crime is intricately connected: corruption. A large part of ESG is about protecting the environment. One of the biggest macroeconomic trends right now is about going carbon neutral. The cornerstone of carbon neutrality is the use of renewable energy. This requires the private and public sectors to come together to build green infrastructure. Combine this collaborative effort with the vast sums of money up for grabs to build the infrastructure and reach global carbon neutrality targets by 2050, and you get the perfect breeding ground for corruption. Especially when the International Energy Agency estimates we need USD 5 trillion of energy investment globally by 2030 to achieve carbon neutrality by 2050.

FATF is vocal in this space, too, having recently released guidance on the illegal wildlife trade. This is in addition to publications on human trafficking, illicit mining, and labor exploitation. In 2023, we'll see more action where ESG and financial crime compliance are interwoven—action like never before—taking one step closer to stopping financial crime.

Conclusion

Luckily, there is hope. If these predictions come true in 2023, it will make it harder for the criminals to hide in the shadows and make our job of stopping them easier. In 2023, technology advances will also materialize allowing the industry to identify more threats than ever before. Advances in transaction monitoring, the greater use of AI and machine learning, including network analytics, and greater focus on perpetual KYC will enable us to take the fight to the criminals. Together, we can make a difference. Feel free to reach out to strategize around identifying truly suspicious activity.