Conclusions

Financial Crime (in its broad sense, including money laundering, terrorist financing, breach of economic sanctions, bribery and corruption, fraud and market abuse) continues to be a major threat for the financial sector across world, and in particular money laundering as one of the areas to pay more attention to. According to the United Nations Office on Drugs and Crime, the amount of money laundered globally in a year is estimated to reach between 2% and 5% of global GDP, or between $800 billion and $2 trillion in current US dollars. With less than 1% of it ever seized or frozen by law enforcement agencies.

Financial Institutions, regulators and crime agencies are working together to leverage upon stronger computational capacity, more advanced mathematical modelling, increased awareness at senior level and stronger coordination to fight Money Laundering across jurisdictions to combat this economic crime.

In this context, financial institutions are investing in improving their capabilities to be able to identify, manage, measure, control and monitor their risks:

1. Framework and Governance, with more formal and comprehensive risk assessments, more granular standards and policies, a better defined and more coordinated three lines of defence model and, more integrated approaches for Risk Management (across different economic crime risks).

2. Organizational structure, with specialized, fully devoted teams led by subject matter experts in the field. Also the centralization of capabilities to ensure efficient and effective action, and the strategic workforce planning that ensures not only the current supply of subject matter experts, but the identification of future needs of skills (e.g. data

scientists). Financial institutions are also investing heavily in ensuring adequate internalisation of the right culture and behaviors to tackle this crime.

3. Business processes, including firm-wide risk assessments as well as individual customer due diligence and risk assessment. Also the investment in streamlining and strengthening the Transaction Monitoring, sanction and payment screening, alert management investigation as well as the engagement with law enforcement.

4. Improvement of the underlying data fabric that supports risk identification and measurement, including improved data sources, better data quality and data governance capabilities.

5. Investment in the technological infrastructure, with specific focus on being able to cope with new threats such as money laundering through cryptocurrencies, in addition to increasing capabilities and automating the technological processes.

One of the main areas of investment, which is also proving to be one of the most effective, is the development of advanced analytics modelling to increase the effectiveness of the detection of threats. That is one of the pillars of the future of an effective money laundering (and broader financial crime) function: one where data, advanced analytics and modelling are able to identify patterns close to real time and trigger productive alerts and automated responses.