ankura

SPECIAL REPORT February 2022

CORPORATE FRAUD

Q&A:
Anti-money laundering challenges in Asia-Pacific

FW discusses anti-money laundering challenges in Asia-Pacific with Marie Gervacio, Michael Peters and Andrew Pimlott at Ankura.

THE PANELLISTS

Marie Gervacio
Senior Managing Director
Ankura
T: +852 2233 2512
E: marie.gervacio@ankura.com

Marie Gervacio is a senior managing director at Ankura, with over 20 years of consulting and audit experience in the financial services industry. She is based in Hong Kong and has served clients throughout Asia-Pacific since 2004. She primarily focuses on governance, enterprise risk & internal control, and financial crime risk management, and is a frequent event speaker and panellist at industry body forums and client workshops in Hong Kong and across the region.

Michael Peters
Senior Managing Director
Ankura
T: +49 17138 0500
E: michael.peters@ankura.com

Michael Peters is a senior managing director at Ankura, based in Germany. He has more than 35 professional years of experience and is a longstanding expert in the field of investigations and prevention of money laundering, terrorist financing and other criminal offences. He has headed nationwide Solution Anti-Financial Crime (AFC) units and was a former investigator of the Federal Criminal Police Office (BKA) and the deputy head of the Financial Intelligence Unit Germany.

Andrew Pimlott
Senior Managing Director
Ankura
T: +971 52859 4433
E: andrew.pimlott@ankura.com

Andrew Pimlott is a senior managing director at Ankura. He is a financial services expert having previously led financial crime investigations across the US, Europe and the Middle East. He has led his clients, large financial institutions, through exceptionally complex and impactful regulatory and legal matters, and has on numerous occasions represented them before the US New York DFS, Treasury/OFAC, DOJ and FBI, as well as EMEA regulators.

FW: Could you provide a general overview of money laundering activity in the Asia-Pacific (APAC) region? What trends have you observed in recent years?

Gervacio: A much more concerted effort to combat financial crime in the region began after the global financial crisis, with many regional regulators enacting revised requirements for licensed financial institutions (IFIs) to enhance anti-money laundering (AML), counter-terrorist financing (CFT) and sanctions screening measures. Recent trends can be viewed in two ways: trends among those attempting to commit financial crime and trends among those working to prevent it. For the former, trends have been increasingly centred around emerging financial technologies related to online banking and payments platforms, as well as cryptocurrency. For those on the prevention side, this has increased the need for finance professionals who are also experts in data, payments systems and cryptocurrency platforms – and their related vulnerabilities. While this has meant a scramble for management and operational talent across Asia-Pacific (APAC), it has also increased demand for board-level experts who can ensure that financial crime and emerging technologies are understood and addressed strategically.

FW: To what extent has the coronavirus (COVID-19) pandemic increased the opportunities for money laundering, particularly with the mass shift to remote working?

Pimlott: As the coronavirus (COVID-19) pandemic continues, the change in people's lifestyle, particularly with the shift to remote working and people moving online, has impacted FIs' ability to detect illicit transactions and contributed to an increase in money laundering. The pandemic has resulted in new and increased cases of counterfeiting of medical goods, investment fraud, adapted cyber crime scams and exploitation of economic stimulus measures put in place by governments. The proceeds of these illicit activities are being laundered by criminal gangs using more complex layering techniques. According to the Financial Action Task Force (FATF), a significant number of jurisdictions around the world report a continued increase in money laundering and cyber-related scams, in particular email and SMS phishing schemes relating to fake links to government stimulus packages, fake distributing aid, infection rate maps and websites selling nonapproved masks.

Gervacio: We understand that opportunities to perpetrate money laundering have increased due to a certain level of fatigue being felt by FIs' compliance professionals. In these cases, there is not a deliberate attempt to weaken internal controls, but rather, the effects of prolonged working hours given the ability to work from remote locations. Specifically, compliance staff may be at risk of not identifying certain instances of suspicious activity, inaccurate information, incomplete files or other flags that indicate that customer identities or transactions may not be trustworthy. In APAC, this is particularly significant, given that FIs typically manage risk across several jurisdictions that vary widely in maturity and complexity, and where the opportunity for financial crime has been exacerbated by unemployment and other economic stress from prolonged COVID-19-related border closures and safety measures.

FW: What legal and regulatory developments have been aimed at tackling money laundering across APAC? To what extent have authorities increased their anti-money laundering (AML) monitoring and enforcement efforts?

Gervacio: Given the spectrum of financial market maturity and complexity across APAC, anti-financial crime professionals in the region are often faced with varied regulatory requirements and standards that present unique challenges in each operating jurisdiction. In general, a more consistent 'high water mark' has been achieved over the past 10 years, where the

> THERE IS AN INCREASING PROPENSITY TO APPLY ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) TO EFFECTIVELY MANAGE FINANCIAL CRIME RISK.
>
> ANDREW PIMLOTT
> Ankura

FATF and other internationally recognised best practices have been adopted into local legal and regulatory frameworks in most major APAC jurisdictions, though there are deficiencies that persist in certain jurisdictions which weaken the ability to implement or enforce some anti-financial crime measures. In more mature jurisdictions in APAC, regulators have maintained their scrutiny of systems of internal control that are designed to prevent and detect financial crime, with an increased focus on governance – in particular, regulators are increasingly focused on the risk culture at FIs and its relationship to whether financial crime risks are higher as a result.

FW: What solutions are being deployed by companies in the APAC region to tackle money laundering? To what extent is technology being used to enhance processes, warnings systems and controls?

Pimlott: There is an increasing propensity to apply artificial intelligence (AI) and machine learning (ML) to effectively manage financial crime risk. We have noticed banks in APAC increase the use of external information and data integration in their AML/CFT systems, supported by more advanced technology, demonstrating stronger capabilities to identify higher-risk relationships, suspicious transactions and networks. According to the FATF, the adoption of innovative technology, such as application programming interface and distributed ledger technology, data standardisation and machine-readable regulations is making it easier and more cost-effective for banks and FIs to build and maintain robust AML solutions. For example, transaction monitoring using AI and ML tools is already allowing regulated entities to carry out traditional functions with greater speed, accuracy and efficiency. However, investing in the latest AI/ML solutions will not result in the desired reduction in financial crime risk without cohesive, well-functioning, experienced in-house teams.

> IN TERMS OF EFFICIENCY AND EFFECTIVENESS, THE COMBINATION OF TECHNOLOGY AND EXPERTISE APPEAR TO BE ESSENTIAL FOR ESTABLISHING SUSTAINABLE AML CONTROLS.
>
> MICHAEL PETERS
> Ankura

FW: Do you believe companies need to enhance the due diligence and background checks they carry out on their business partners and customers?

Peters: Despite continued efforts to improve know your customer (KYC) and AML practices, FIs and industries across the globe had to pay record-breaking fines in recent years due to shortcomings in this field. This emphasises once again the essential role of proper AML compliance and that further steps for establishing robust KYC and know your employee (KYE) processes need to be taken by companies to avoid financial and reputational damage. These steps include the implementation and continuous development of such measures as AML due diligence, background checks, and third party and applicant due diligence. It is important to bear in mind that an efficient and effective KYC and KYE process is the basis for compliance with regulations. It minimises the risk of companies becoming involved in money laundering and ensures that services are used accordingly. Hence, it enhances safety for all parties involved – the obliged party and its employees, customers and business partners.

FW: What advice would offer to companies on establishing AML controls that can detect suspicious activities and serve as an effective red flag system?

Peters: In terms of efficiency and effectiveness, the combination of technology and expertise appear to be essential for establishing sustainable AML controls. The rapidly changing world – a drastic shift toward digitalisation due to COVID-19, the increasing popularity of cryptocurrency and virtual assets, continuous growth in the volume of cross-border transactions – demands from companies a constant optimisation of transaction monitoring and screening processes and digital tooling. Thus, it is essential to create an environment that enables the timely update of existing tools, prompt implementation of new technical solutions, such as advanced ML and advanced data analytics technologies, among others, as well as the development of responsible expertise. In turn, this will

bring AML practices to the next level. Another key enabler to assess multiple transactions is data. The more and higher quality data available, the easier it will be to detect suspicious activities. The first step toward a unified transaction monitoring utility has already been taken – the Dutch pilot data utility platform. Lastly, a company's AML landscape is only as strong as its weakest link. Therefore, constant assessment of AML processes is key to improving financial crime risk management.

FW: How do you envisage the fight against money laundering in the APAC region developing in the months and years ahead? Are you optimistic about the prospects for improved systems that lead to a drop in financial crime?

Gervacio: Despite the expenditure of significant time and resources in APAC over the past decade, financial crime continues to be a key risk for regional FIs. As recently as November 2021, significant fines were levied against four major banks in Hong Kong for failures to carry out appropriate customer due diligence procedures. This is indicative of the fact that challenges remain with respect to operational effectiveness, and the knowledge, experience and training of anti-financial crime teams, combined with increasingly sophisticated technology that puts more powerful tools into the hands of money launderers and other financial criminals. However, the same level of technological innovation should enable stronger monitoring of data and transactions on a real-time basis, reducing unnoticed or latent information that previously provided opportunities to perpetrate financial crime. Investments in technology itself and technology talent should be the biggest priority to combat financial crime in 2022 and beyond. ■

"INVESTMENTS IN TECHNOLOGY ITSELF AND TECHNOLOGY TALENT SHOULD BE THE BIGGEST PRIORITY TO COMBAT FINANCIAL CRIME IN 2022 AND BEYOND."

MARIE GERVACIO
Ankura

FINANCIER WORLDWIDE corporatefinanceintelligence