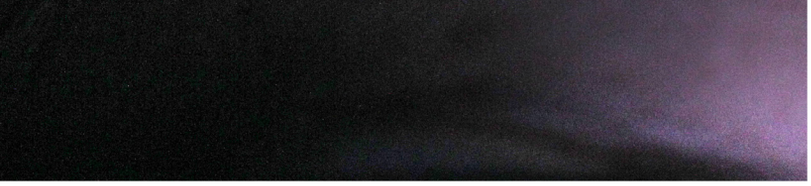
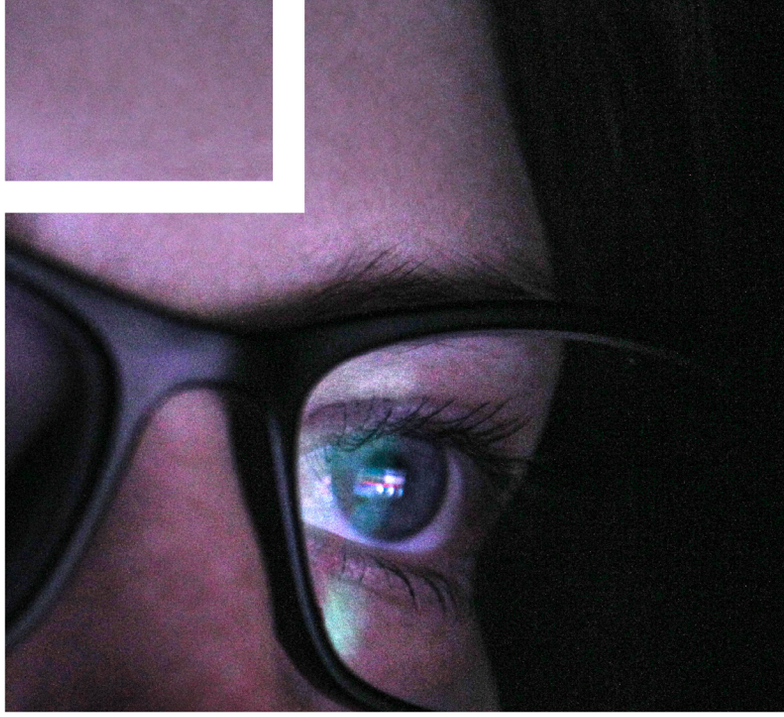
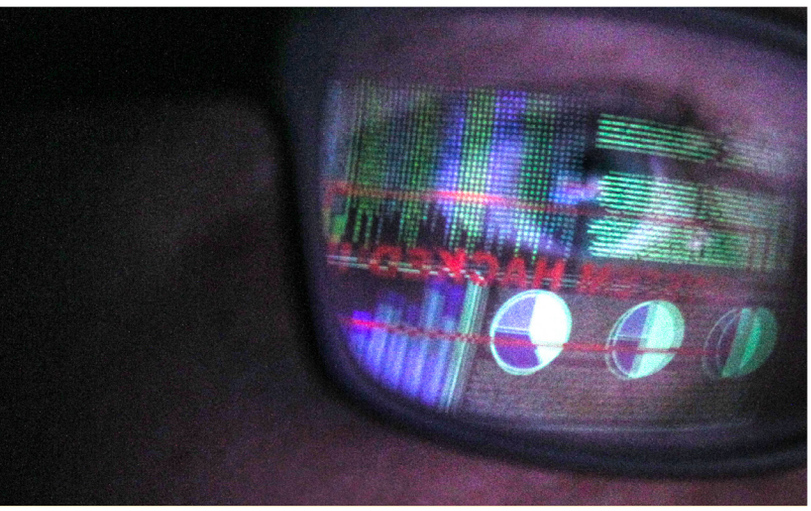
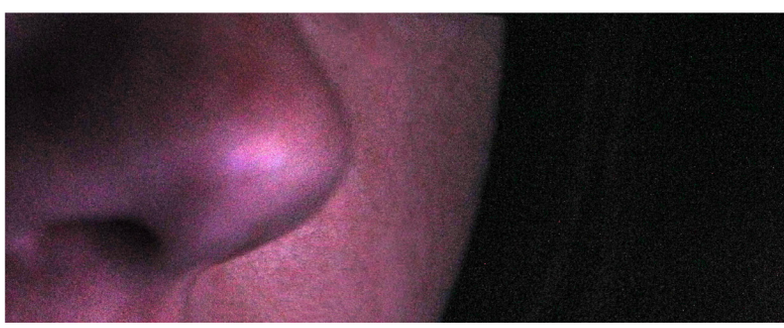






The fight against money laundering



In recent years, organisations in many parts of the world have been pouring funds and resources into headcount and technology to fulfil ever more stringent global and local standards on anti-money laundering (AML). Organisations in Asia in particular are responding to the general pivot towards more proactive local regulatory scrutiny of AML and financial crime controls. The FATF Mutual Evaluation, of which includes the on-site inspection which was recently completed in Hong Kong, also guided jurisdictions to identify their weaknesses and move towards to international standards. While these standards and reviews help shape organisations' frameworks to prevent and detect fraud and economic crime, criminals continue to pose threats against organisations with new creative ways of committing illegal activities and cleaning their dirty money.

According to the Hong Kong Money Laundering and Terrorist Financing (ML / TF) Risk Assessment Report ('the Report') issued recently by the HKSAR Government, nearly 80% of money laundering cases were associated with fraud and forgery during the years 2011 to 2015. A high exposure to dealing with fraud-related proceeds comes as no surprise, as Hong Kong handles substantial cross-border payments and settlements on a day-to-day basis. Coupled with a high degree of free trade and its financial secrecy provisions, this environment has attracted domestic and international offenders to abuse the banking system, posing high money laundering risk to the banking sector in Hong Kong.

In the face of the battle against money launderers, what can be done to turn this battle around? What can be done to better manage money laundering risk? Here are three questions organisations should ask themselves, and why.

Lead your army in the right direction – Do organisations fully understand their risk exposure?

Identify the true culprits – Have organisations thoroughly analysed their existing customer information?

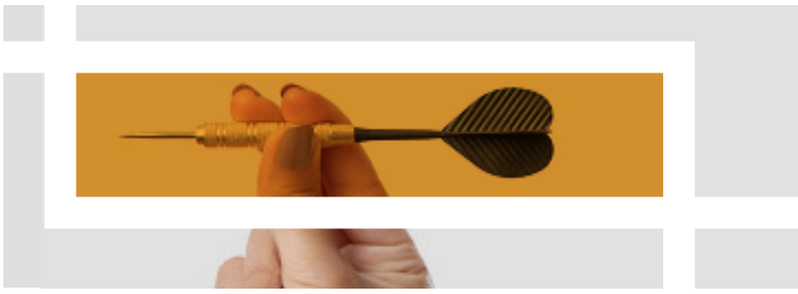
Sharpen your weapon – Are organisations' systems truly up to the task?

pwc

Lead your army in the right direction – Do organisations fully understand their risk exposure?

Many financial institutions have noted how they have invested abundantly into technologies when reacting to fraud and economic crime incidents. However, they seem to have less concern in actively searching for loose ends. According to the 2018 PwC Global Economic Crime Survey, slightly more than half of the organisations in the financial services sector located in Asia-Pacific say they have performed risk assessments on AML in the past two years. Also, as one of the findings identified in the fourth round of the Financial Action Task Force's (FATF) Mutual Evaluations performed so far, risk assessments conducted by financial institutions in some of the jurisdictions are not comprehensive enough and do not cover all activities, products and services, resulting in weak implementation of preventive measures. With the recent revision of the AML Guidelines issued by the Hong Kong regulators, the importance of understanding one's risk exposure becomes even more relevant as regulators reinforce their expectation on financial institutions to develop their front-to-end AML / CFT Systems under a risk-based approach. Without appropriate risk assessments, organisations tend to plan the wrong strategy due to limited knowledge and lead their armies in the wrong direction for battle, leaving the weakest links of the organisations exposed to exploitation.

Practically speaking, understanding one's risk exposure helps organisations enforce risk-based measures and implement more relevant policies and procedures when managing and mitigating risks. This is particularly so in setting out risk mitigation controls and tolerance levels for high risk situations when performing processes such as customer due diligence, customer risk rating and transaction monitoring. Organisations will also gain efficiencies when determining levels of resources to allocate to the respective processes based on risk exposures.



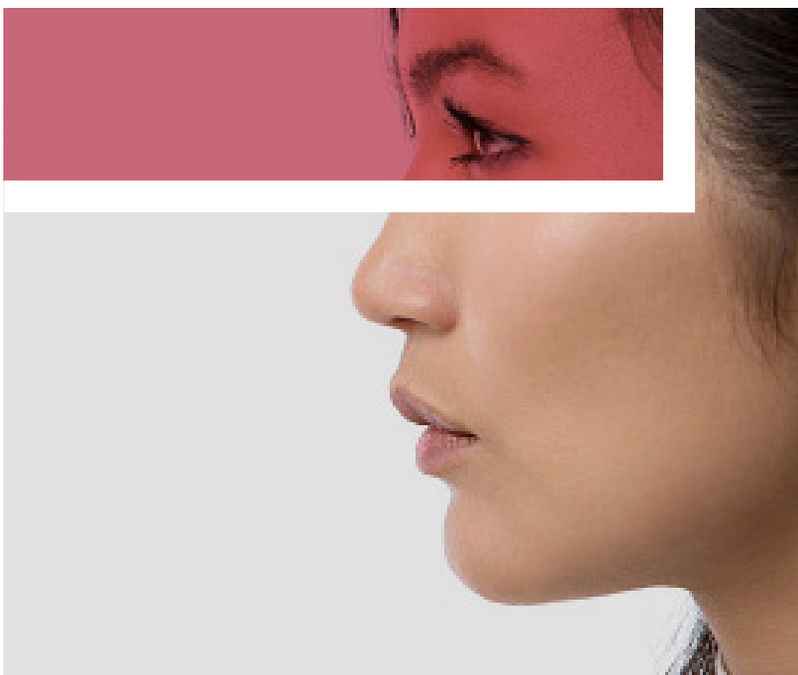
Identify the true culprits – Have organisations thoroughly analysed their existing customer information?

One of the key challenges faced by the Hong Kong banking sector is that local bank accounts have been used as conduits for proceeds generated from fraud committed in multiple overseas jurisdictions.

According to the Report, the most significant threat consists of typologies whereby bank accounts are opened by non-residents and/or corporates domiciled in jurisdictions outside of Hong Kong. These corporates have no physical nexus to Hong Kong nor apparent business ties to the city. Criminals have also evolved to better conceal the ownership and control of their illicitly obtained assets through obscure beneficial ownership, as well as by recruiting professional money launderers in the money laundering process. Organisations have repeatedly noted that their KYC processes are already extremely detailed, if not cumbersome – so what is missing from the organisations to identify the actual culprits?

Faced with the difficulty of identifying beneficial ownership, financial institutions should not focus on merely adding a few more checkboxes to the lists of documents to be obtained. Lengthy checklists not only bring inefficiency to the process, they also lead to the probable result of rejecting 'good' customers whilst overlooking the real risk within the organisation, hurting both customer experience and the overall business. Rather, as suggested by a recent FATF publication on beneficial ownership, organisations can consider conducting analytics based on information already received to identify activities and trends which are indicative of concealment of beneficial ownership. For example, where the identity of beneficial owners cannot be ascertained, analysis of the management structure as well as financial dealings of the management personnel can help organisations assess whether senior management or any third party is exerting control over the company. Analytics can also be performed on contact information provided by customers to identify common addresses or telephone numbers, which can shed insight on whether customers are shell companies as they will need directorship, company management services and the use of professional nominees.

On the front of enhancing the transparency of beneficial ownership of corporate entities, more and more authorities are imposing additional requirements with regards to the disclosure of beneficial ownership information. Some of the more recent developments include Mainland China requiring banks to submit recorded information of beneficial owners to the People's Bank of China since 2017. All companies incorporated in Hong Kong have been required to maintain up-to-date beneficial ownership information by keeping registers of significant controllers since March this year. Also, the European Parliament adopted the 5th AML Directive which requires Member States to ensure registers of ultimate beneficial owners of companies and other legal entities become accessible to the general public.



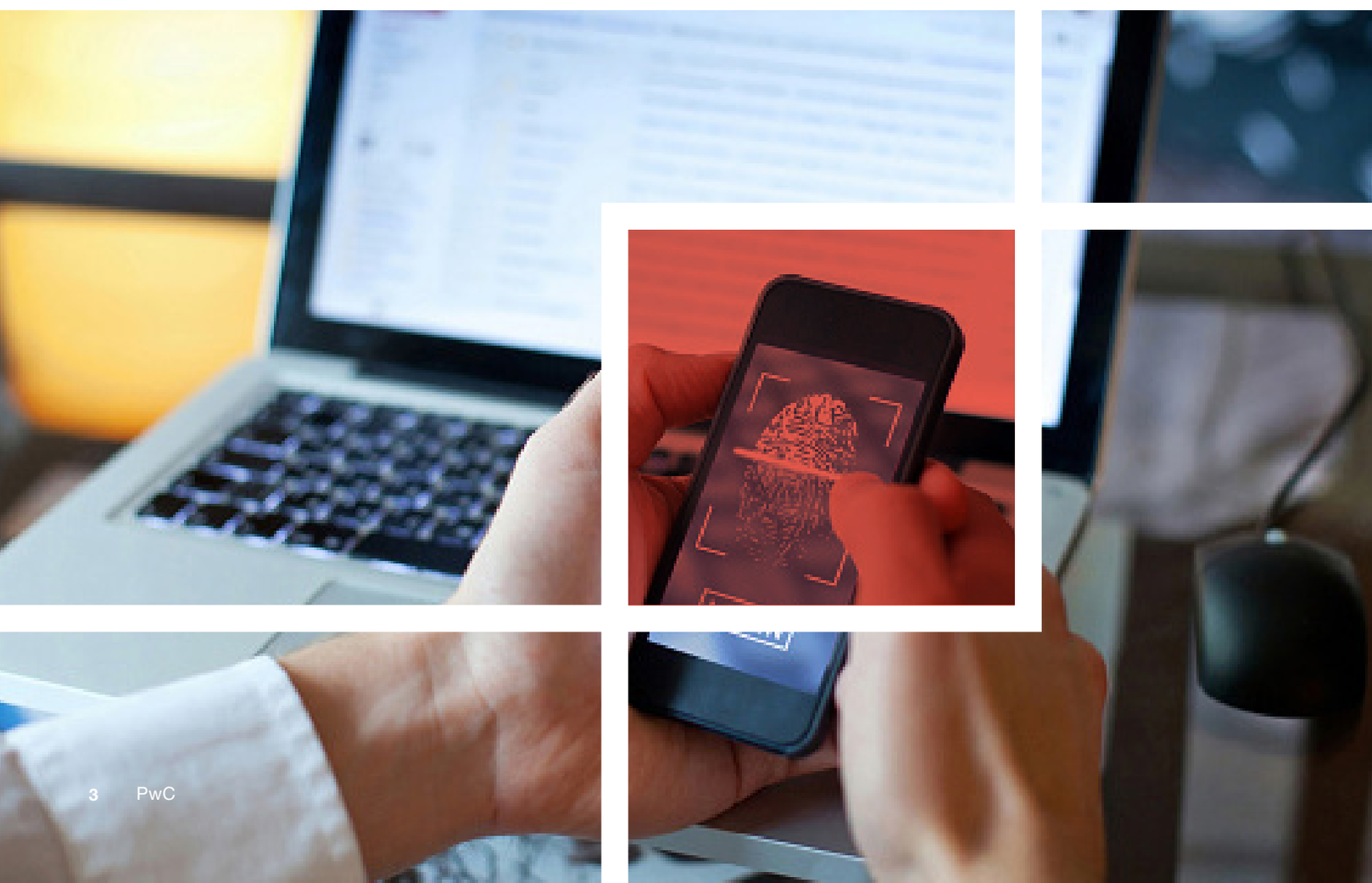
Sharpen your weapon – Are organisations' systems truly up to the task?

As mentioned earlier, financial institutions are increasingly incorporating a variety of technologies into compliance programmes to manage their money laundering risk. There is also a general demand to manage risks in a more efficient way by convergence of AML, cybercrime and fraud controls. This, however, is not without challenges. With so many new technologies and tools available in the market, banks have found it difficult to assess the suitability of these technologies against their business requirements. At the same time, there are banks that have not considered a full range of criteria when deciding which system to implement. In general, it is common for organisations to rely heavily on the system vendor from system implementation and configuration to filter and threshold setting, without taking their own needs into account. Organisations also do not always perform thorough reviews of design and operational effectiveness pre and post system implementation.

As an international and regional trading hub supporting cross-border trade transactions, operating AML / sanctions systems in an efficient and effective manner is particularly pivotal and relevant to banks located in Hong Kong. The result of relying on an ineffective system could be detrimental. Multiple organisations have frustrations with system parameters that do not suit their business and thus generate too many alerts with false positive hits. At the other extreme, there are some systems that generate low volume of alerts because the thresholds are not tailored to the nature of their transactions and clientele. Either way, investment in these systems goes to waste as they are not capturing the suspicious activities they are supposed to. The Thematic Review of Authorised Institutions' Sanctions Screening Systems issued by the Hong Kong Monetary Authority (HKMA) April this year also identified the above weaknesses in Sanctions systems and required banks to perform on-going monitoring, tuning and testing on their systems that support Sanctions compliance programmes. Recent regulatory disciplinary actions on deficiencies of monitoring business relationships further highlight the importance of the effectiveness and efficiency of AML systems within financial institutions when detecting and preventing money laundering activities.

One of the concerns around system effectiveness is data quality. No meaningful results can be generated and relied upon if banks cannot ensure the completeness and accuracy of the data being fed into and generated by the AML / sanctions systems. Moreover, senior management needs to play a more active role to ensure the level of monitoring and screening performed is aligned to the business profile and risk exposure of the bank. Senior management also ought to recognise that given the constant change in the AML / sanctions space, the assessment of system performance requires continuous effort and should be performed regularly and frequently.

Appropriate documentation of the systems in place has also proven its importance in establishing standard operating procedures an d evidencing the testing / tuning procedures performed. It also helps address some of the regulator's concerns around the documentation of the rationale for system configurations and allocation of roles and responsibilities.



It is not a one-man battle

The fight against money laundering has never been static – unfortunately it is becoming even more challenging with criminals relentlessly developing new schemes and expanding the battleground into the virtual territories. The good news is, organisations will be able to strengthen their fight against money laundering by being vigilant about where and who the culprits are and sharpening their weapons accordingly. The even better news is that organisations do not have to fight this alone. With growing networks and allies built through information sharing initiatives within the private sector, between the private and public sectors as well as between jurisdictions, organisations can further step up their compliance efforts while leveraging the strengths of others.

Contact us

Mary Wong

Partner, Forensic Services
PwC Hong Kong
+852 2289 2587
mary.wong@hk.pwc.com

Jessica Li

Associate Director, Forensic Services
PwC Hong Kong
+852 2289 2522
jessica.ka.li@hk.pwc.com

www.pwchk.com

This article was first published by the Hong Kong Institute of Bankers on '*Banking Today*', issue no.102.