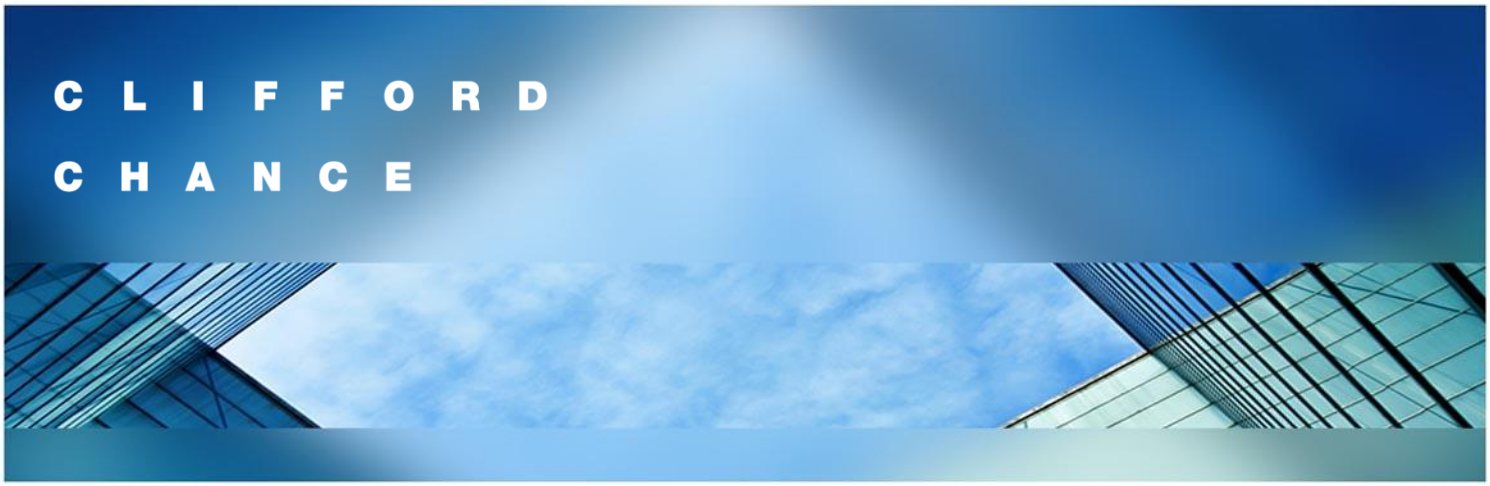


# HKMA PENALISES FOUR BANKS HK$44.2 MILLION FOR MONEY LAUNDERING CONTROL FAILURES: KEY TAKEAWAYS

On 19 November 2021, the Hong Kong Monetary Authority (HKMA) announced that that it had completed investigations and disciplinary proceedings against four banks under the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Ordinance (Cap. 615) (AMLO), imposing pecuniary penalties of a total of HK$44.2 million. This arose from a series of onsite examinations the HKMA conducted on banks' systems and controls for compliance with the AMLO after its enactment on 1 April 2012. Common control lapses identified relate to ongoing monitoring of business relationships through customer due diligence (CDD) and deficiencies in conducting enhanced CDD in high-risk situations. Banks should reference these examples to review data quality and transaction monitoring system effectiveness, and take appropriate risk mitigating measures on an ongoing basis. The HKMA expects up-to-date understanding of evolving risks, responsible regtech adoption (particularly in CDD and transaction monitoring) and close collaboration in the ecosystem. These are areas of consistent regulatory emphasis and we summarise key recent guidance below.

**Quick read**

- These latest fines imposed by the HKMA reiterate that the Hong Kong regulators are serious about AML and want to send a clear deterrent message; they are in line with the SFC's penalties for money laundering internal control failures in the past few years
- Industry understanding and experience not being mature is not an excuse; banks should keep themselves up to date as risks emerge and evolve
- Collaboration among industry participants and public-private partnership is expected in combating fraud and ML
- Attention should be paid to customer monitoring not only during account opening - it must be continuous and timely
- Good quality data is key and banks should review data quality by reference to these case examples
- Where ML and TF risk is high, additional diligence is required and senior management should be involved
- Responsible adoption of regtech is also important in enhancing AML processes

## INTRODUCTION

The HKMA announced on 19 November 2021 that that it had completed investigations and disciplinary proceedings against four banks under the AMLO, imposing pecuniary penalties of a total of HK$44.2 million. The HKMA also issued orders for an independent external advisor to assess and report to the HKMA on the sufficiency and effectiveness of remedial measures taken by two of the banks to address identified contraventions and other deficiencies.

The common control lapses identified in various periods between April 2012 (when industry understanding and experience were less mature) and September 2018 relate to ongoing CDD, and enhanced CDD in high-risk situations. The HKMA notes that since then, significant progress has been made by the industry, including the banks concerned, in enhancing financial

crime compliance capabilities, with attention being given to improving processes, controls, and staffing.

This follows a series of money laundering (ML) enforcement cases by the Securities and Futures Commission (SFC) between 2019 and 2021, including the case involving the high profile 1Malaysia Development Berhad (1MDB) scandal, which led to the largest ever single fine (of HK$2.7 billion) imposed by the SFC and fines otherwise ranging from HK$3.7 million to HK$25.2 million.

Significant autonomy is given to regulated financial institutions in terms of design and implementation of their AML compliance programmes. There is no "one-size-fits-all" when it comes to ML controls, which should be commensurate with the financial institution's size, services offering, customer profile and geographical footprint. Finding the right balance in a risk-based fashion, between practicality and cost-effectiveness, in detecting ML, is a constant challenge. Disciplinary actions like these are therefore invaluable from which to learn lessons.

## SUMMARY OF HKMA FINDINGS

The issues identified by the HKMA are set out in more detail in tabular form at the end of this briefing. In summary:

- The four banks were found to have failed to comply with their duty to continuously monitor customer business relationships through ongoing CDD. These notably included lack of timely periodic reviews (in some cases, for high-risk customers). One bank was found to have adopted a "mailer approach" under which the bank issued a letter to customers enquiring whether there had been any change in the customer information provided at account opening and, if the customer did not respond within 21 days, the bank assumed that there had been no change and no follow-up review or verification steps were taken – such approach was considered by the HKMA to have "inherent deficiencies" and did not ensure customer information was up to date and relevant.
- In situations where the HKMA perceived high ML and terrorist financing (TF) risks, there was an identified lack of reasonable measures to establish their customers' or their beneficial owners' sources of wealth and funds, or obtain senior management approval to establish or continue the business relationship. One bank was also found to have delayed in implementing these measures after obtaining knowledge that their customers or their beneficial owners were politically exposed persons (PEPs).

## FACTORS CONSIDERED BY HKMA TO DETERMINE DISCIPINARY ACTION

It is further notable that in determining its disciplinary action, the HKMA took into account that the banks had taken remedial and enhancement measures to address the deficiencies identified by the HKMA, had co-operated, and had clean AML-related disciplinary records, but balanced this against the seriousness of the investigation findings and the need for deterrence.

## KEY TAKEAWAYS FOR BANKS

The four banks' contraventions principally spanned from April 2012 to September 2017, with record keeping contraventions extending up to September 2018. The HKMA notes that this was when the industry's "understanding and experience was less mature". By the time of publication of the Financial Action Task Force (FATF) Mutual Evaluation Report (MER) on

Hong Kong on 4 September 2019, based on an onsite visit from 31 October to 15 November 2018, Hong Kong was found to be overall compliant and effective in respect of its AML and CTF systems.

Nonetheless, the HKMA's also stressed that whilst significant progress has been made by the industry, including by the banks concerned, banks should make reference to these examples to review data quality and transaction monitoring system effectiveness, and take appropriate risk mitigating measures on an ongoing basis. The HKMA expects up to date understanding of evolving risks, use of better-quality data, responsible innovation including regtech adoption and close collaboration in the ecosystem.

Use of better quality data, responsible adoption of regtech and keeping up to date and collaboration are consistent messages which the HKMA has emphasised in recent publications:

- **Responsible regtech adoption.** In a circular in August 2021, the HKMA highlighted the FATF July 2021 report on opportunities and challenges of new technologies for AML, which discusses how new technologies such as machine learning and natural language processing can improve the speed, quality, and effectiveness of AML measures. In line with global trends, the HKMA has been taking steps to support AML innovation. This began with industry engagement and conversations with about 40 banks regarding their approach in adopting regtech to enhance AML processes culminating in a report in January 2021 sharing their experiences. The report provides technology spotlights, and guidance on addressing common operational challenges such as data and process readiness; executive support and stakeholder buy-in; and working with third party vendors.
- The subsequent July 2021 Regtech Adoption Practice Guide helps banks to assess whether they have appropriate governance, controls, skills, infrastructure and underlying data to enable them to apply regtech solutions that assist AML efforts in the area of ongoing monitoring of customers.
- **CDD including where customers onboarded remotely.** The HKMA issued guidance regarding remote customer onboarding in February and August 2019, as well as September 2020, allowing banks to employ appropriate technology solutions to mitigate the risks when identifying and verifying the identity of an individual customer, corporate customer representative or beneficial owner, and expects that any technology solutions adopted should be at least as robust as those performed when the individual is in front of the staff of a bank. Examples of good practices were provided in June 2020 following a thematic review of AML control measures for remote customer onboarding. Good practices include that it is essential for banks which rely on "off-the-shelf" solutions to demonstrate an appropriate level of understanding of how the solutions work. Other good practices include due diligence of the vendor's capability and reliability, and ongoing quality assurance processes on the technology deployed. For more discussion on this topic, see our RIFC blog post here.
- The AML / CTF Guideline for authorised institutions revised in October 2018 endorses the use of commercially available databases for screening whether customers, their beneficial owners and connected parties are PEPs, and the source of wealth and funds of high-risk customers, as well as the use of sophisticated name screening systems against terrorist/sanction designations as examples of good or reasonable AML practices adopted by

banks. The HKMA stresses that a bank should be aware of a database's fitness for purpose and limitations depending on the source of the underlying data including whether it only encompasses publicly available information, the definition of PEP used and any deficiency in technical capability. Appropriate measures should be taken to ensure the completeness and accuracy of commercial databases of terrorists and designated parties, for example, by conducting periodic sample testing.

It is important to get PEP identification and associated CDD right, as disciplinary action has been taken by the HKMA for PEP related failures in the past. In April 2017, Coutts & Co AG was fined HK$7 million for contravening the AMLO. Similarly, the State Bank of India had earlier been fined HKD7.5 million.

- **Transaction monitoring, use of quality data and close collaboration in the ecosystem**. The HKMA issued a circular in April 2021 following its thematic review of banks' use of external data and data and network analytics to effectively identify high risk relationships and suspicious transactions including mule account networks (i.e. linked accounts that are not genuine customer accounts and potentially used for ML). The importance of senior management support; intelligence sharing within the institution and any wider group; and performance evaluation of the use of data analytics and external data in an AML compliance programme were emphasised. For more, see our RIFC blog post here.
- The June 2020 edition of the HKMA's Regtech Watch newsletter highlighted regtech use cases in transaction monitoring and suspicious activity reporting including the use of supervised machine learning to tackle the problem of high false positives and the application of advanced data mining techniques to expanded data pools to trace and identify networks of transactions and counterparties associated with customers. The HKMA has further provided guidance such that a bank should be conversant with the abilities of the algorithm used in its transaction screening system, with particular attention being paid to the ability of the name screening system to identify names with minor alterations such as names in reverse order, partial names and abbreviated names.
- A May 2018 circular and guidance paper gave pointers for improving the quality and consistency of suspicious transaction reports (STRs). The circular also referred to the Fraud and Money Laundering Intelligence Taskforce (FMLIT), which involves collaboration between the Hong Kong Police Force, HKMA, Hong Kong Association of Banks (HKAB) and a number of banks, and has an alerts function to disseminate typologies and sanitised intelligence to banks, so that they can identify risks and trends early, and make more informed, risk-based decisions regarding their AML processes including applying risk indicators to CDD and ongoing monitoring and review.

## Position in APAC

- **Singapore**. Similar themes are playing out in Singapore. The sharing of data and adoption of regtech are being encouraged. Singapore has a FMLIT equivalent to facilitate public-private information exchange, which includes the Anti-Money Laundering and Countering Financing of Terrorism Industry Partnership (ACIP), made up of the Commercial Affairs Department (CAD) of the Singapore Police Force, Monetary Authority of Singapore (MAS),

Association of Banks Singapore and various banks. MAS has further announced a digital sharing platform known as Collaborative Sharing of ML and TF Information and Cases (COSMIC), expected in the first half of 2023 and which will be operated by the MAS. This will enable banks to warn one another about unusual activity in customers' accounts with the stated aim of closing the gap currently exploited by financial criminals to make illicit transactions through accounts of different entities in different banks such that each bank does not have sufficient information to detect these transactions. While some other countries have introduced arrangements for information sharing among financial institutions, the COSMIC platform will be the first centralised platform where information is shared in a structured format that allows for seamless integration with data analytics tools. In terms of encouraging the adoption of regtech, MAS has facilitated experience sharing, provided guidance, and committed funds. In the MAS' Guidance for Effective AML/CTF Transaction Monitoring Controls in September 2018, it encouraged the use of new technology and data analytics to improve transaction monitoring outcomes. At the end of 2018, ACIP's Data Analytics Working Group launched a paper to share the experiences of ACIP member banks in using data analytics techniques to combat financial crime discussing use cases, key challenges and potential solutions in adoption of such tools. In September 2020, the MAS issued a paper following thematic inspections on private banks and set out its supervisory expectations of effective AML controls, which include the use of credible commercial databases. In August 2020, MAS committed S$250 million (about US$183 million) over three years under the enhanced Financial Sector Technology and Innovation Scheme (FSTI 2.0) to accelerate technology and innovation-driven growth in the financial sector including use of technology to combat ML.

- **Australia**. A series of high profile AML enforcement outcomes against major Australian financial institutions in recent years has meant the Australian Transaction Reports and Analysis Centre (AUSTRAC) is arguably Australia's most feared regulator. In 2020, the regulator achieved the highest ever corporate penalty in Australian history with a fine of AUD1.3 billion imposed on Westpac for systemic failings in its AML/CTF framework. In December 2020, the Australian government passed legislation (which came into effect from 18 June 2021) implementing the Financial Action Task Force's recommendations following its mutual-evaluation report on Australia's AML/CTF regime, including in relation to customer identification procedures, information sharing and cross-border payments. In 2017, AUSTRAC established the Fintel Alliance, an information-sharing initiative to increase the resilience of the financial sector to criminal exploitation and support law enforcement investigations into serious crime and national security matters. Emerging financial crime including ML and TF indicators and typologies are shared to facilitate monitoring and identifying and detecting suspicious transactions. In April 2021, AUSTRAC released further resources to encourage submission of higher quality Suspicious Matter Reports (SMRs) including a reference guide and checklist. Australian regulators are also focusing increasingly on the intersection of data and regtech: the Australian Prudential Regulation Authority (APRA) has invested in a new Data Collection Solution and established an Innovation Lab utilising techniques such as artificial intelligence, machine learning, network analytics and natural language processing to analyse its data. The Australian Securities and Investments Commission (ASIC) is also investing significant resources to enhance its ability to monitor and interrogate data

with a view to identifying potential misconduct. Australian regulators have also emphasised their intention to cooperate through information sharing, including in relation to information obtained through market surveillance and market participant reporting.

## CONCLUSION

AML compliance continues to be an area of regulatory focus in Hong Kong. The risk-based approach in AML compliance requires judgment and a balancing act between operational efficiency and appropriate ML controls and procedures; design and implementation can also vary widely depending on the bank's circumstances.

Quality data and regtech are key to striking this balance. Also key is awareness through training, not only of compliance staff, but also front-line staff, who are the first line of defence. Our expert team would be pleased to assist with your AML training and internal control review needs.

## TABLE SETTING OUT AMLO CONTRAVENTIONS OF AND ORDERS IMPOSED ON EACH BANK

| Bank A | Bank B | Bank C | Bank D |
|---|---|---|---|
| **1. Duty to continuously monitor customer business relationships (s5(1), Sch 2, AMLO):** | | | |
| *April 2012 – September 2014*<br><br>Failed to conduct periodic review of customer information to ensure it was up to date and relevant in respect of 148 customers where changes relating to their company name, director and/or shareholder had occurred. The bank adopted an inherently deficient mailer approach by issuing an enquiry letter to customers requesting a response if there had been a change in customer information since account opening. It assumed no change if no response was received within 21 days and did not take follow up or verification steps. | *January 2013 – June 2014 and January 2013 – October 2016*<br><br>Failed to conduct annual reviews for high-risk customers or reviews upon trigger events in a timely manner in respect of 46 customers of the sample reviewed by the HKMA.<br><br>Failed to examine the background and purpose of complex and usually large transactions or transactions which had an unusual pattern or no apparent economic or lawful purpose in respect of 29 customers of the sample reviewed by the HKMA. | *April 2012 – September 2014*<br><br>Unduly delayed conducting periodic review for 87 high risk customers out of line with its policy of annual review of high-risk customers to ensure its existing records were up to date and relevant. | *April 2012 – November 2014*<br><br>Failed to conduct periodic review to ensure customer information was up to date and relevant for 5,725 customers including:<br>• system error in extracting certain customers due for periodic review; and<br>• failure to update and set out in its policy and procedures, specific events to trigger periodic review; effectively communicate procedures to relevant staff; and establish effective monitoring and control procedures to ensure due implementation of policy requirements. |

| Bank A | Bank B | Bank C | Bank D |
|---|---|---|---|
| **2. Establishment and maintenance of effective procedures for continuous customer monitoring (s19(3), Sch 2, AMLO):** | | | |
| *April 2012 – September 2014*<br><br>See above. | *January 2013 – June 2014*<br><br>From its automated transaction monitoring system, alerts were generated for transactions hitting a pre-set threshold, but only a small portion were investigated based on restrictive selection criteria. | *April 2012 – September 2014*<br><br>No automated centralised record (or suitable alternative) or clear practical guidance such that periodic review procedures ineffective for capturing information to enable continuous monitoring of customer business relationships<br><br>. | *April 2012 – November 2014*<br><br>See above. |
| **3. Reasonable measures in situations of high risk of ML or TF (s15, Sch 2, AMLO):** | | | |
| *April 2012 – September 2014*<br><br>Failed to conduct enhanced CDD in respect of 19 pre-existing high risk customers whose accounts had been opened before the AMLO commenced on 1 April 2012. | *January 2013 – June 2014*<br><br>Failed to obtain senior management approval to continue the business relationship in high risk situations in a timely manner with respect to 51 customers of the sample reviewed by the HKMA. | *April 2012 – September 2014*<br><br>Failed to obtain senior management approval to establish or continue the business relationship in high risk situations in a timely manner with respect to 59 customers of the sample reviewed by the HKMA. | N/A |
| **4. Duty to keep records (s20(3), Sch 2, AMLO):** | | | |
| N/A | *February 2013 – June 2018*<br><br>Failed to provide to the HKMA relevant reports based on reviewers' initials and/or annotations with respect to seven customers. | *October 2014 – September 2018*<br><br>Unable to provide HKMA with relevant risk assessment forms of 26 customers. | N/A |

The following issues are specific to **Bank C** only:

**5. Reasonable measures before establishing or continuing customer relationship where knowledge that customer or beneficial owner PEP (s10(1)-(2), Sch 2, AMLO)**

*April 2012 – September 2017:* In respect of a number of existing customers or their beneficial owners that were or had become PEPs, delays for more than seven months after knowledge of their status in obtaining senior management approval or establishing sources of wealth and funds before continuing the business relationship.

**6. Establishment and maintenance of effective procedures for determining whether customers or beneficial owners, PEPs (s19(1), Sch 2, AMLO)**

*April 2012 – September 2014:* Failure to establish effective procedures for determining whether customers or their beneficial owners were PEPs. This was evidenced by substantial delay in PEP batch scanning, a long time being taken to review potential hits and name searches not being conducted properly.

**7. Ordering institution to include in message or payment form accompanying wire transfer certain information (s12(5), Sch 2, AMLO)**

*April 2012 – September 2014:* As ordering institution, failed to include certain originators' information in 1,076 payment messages for outgoing cross border wire transfers (or information included was incomplete).

**8. Establishment and maintenance of effective procedures for identifying and handling wire transfers not compliant with s12(5) (s19(2), Sch 2, AMLO)**

*April 2012 – September 2014:* Failure to establish effective procedures for identifying and handling wire transfers with incomplete information in payment messages.

The following issue is specific to **Bank D** only:

**9. CDD for pre-existing customers involved in certain transactions or where material change in operation of accounts (s6(1)-(2), Sch 2, AMLO):**

*April 2012 – October 2015:* CDD for certain pre-existing customers involved in suspicious transactions took place more than 8 to 22 months after STRs were filed with the Joint Financial Intelligence Unit (JFIU) and the business relationship was not terminated when review was unable to be conducted for 8 to 31 months after STRs were filed.

| Bank A | Bank B | Bank C | Bank D |
|---|---|---|---|
| **Pecuniary penalty (s21(2)(c) AMLO)** | | | |
| HK$6 million | HK$8.5 million | HK$20.7 million | HK$9 million |
| **Independent external advisor assessment and report (s21(2)(b) AMLO)** | | | |
| No | Yes | Yes | No |

CLIFFORD CHANCE

# CONTACTS

**Donna Wacker**
Partner

T +852 2826 3478
E Donna.Wacker
@cliffordchance.com

**Jonathan Wong**
Partner

T +852 2825 8841
E Jonathan.Wong
@cliffordchance.com

**William Wong**
Consultant

T +852 2826 3588
E William.Wong
@cliffordchance.com

**Michael Wang**
Consultant

T +852 2826 3564
E Michael.Wang
@cliffordchance.com

**Kabir Singh**
Partner

T +65 6410 2273
E Kabir.Singh
@cliffordchance.com

**Janice Goh**
Partner, Cavenagh Law LLP

T +65 6661 2021
E Janice.Goh
@cliffordchance.com

**Tim Grave**
Partner

T +612 8922 8028
E Tim.Grave
@cliffordchance.com

**Alexandra Payne**
Senior Associate

T +612 8922 8508
E Alexandra.Payne
@cliffordchance.com



www.cliffordchance.com

Clifford Chance, 27th Floor, Jardine House, One Connaught Place, Hong Kong



Clifford Chance

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.