CLEMENT WONG
YAT-FAI LAM
RONALD CHUNG

ANTI-MONEY LAUNDERING: THE BANKING INDUSTRY IN HONG KONG

Dirty money has no place in our economy, whether it comes from drug deals, the illegal guns trade, or trafficking in human beings. We must make sure that organized crime cannot launder its funds through the banking system or the gambling sector. Our banks should never function as laundromats for mafia money, or enable the funding of terrorists.

- Cecilia Malmström, Former Home Affairs Commissioner, European Union

With financial institutions and professionals at the front line of the battle against money laundering, they played a critical role in preventing criminal money from getting into the financial system. To strengthen its anti-money laundering (AML) efforts the Hong Kong banking regulator, The Hong Kong Monetary Authority (HKMA) issued a guideline to all licensed institutions and persons[1].

The Chief Executive of GCBC[2], a mid-size multinational authorized institution, was one of those who received this guideline. GCBC had served the Hong Kong market for close to half a century. When it first entered the market, it mainly served small to medium corporate clients in support of its headquarters' business. Over the period of its presence in Hong Kong, GCBC had expanded to include Hong Kong based business, primarily Hong Kong companies that served it existing clients; Hong Kong nationals that moved back as well as clients that moved to Hong Kong, e.g., expats from it's home country[3].

Clearly, with a multinational bias in its client portfolio, how to strengthen its AML system presented a big challenge to GCBC's management. At the first level, this meant more resources to be spent on an enhanced compliance system. Secondly, the implementation of this system

[1] A good background to HKMA's guideline to AML can be found in Guideline no. 3.3 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g33.pdf

[2] The character and the financial institution here are fictitious, but do represent a typical scenario encountered by chief executive of financial institutions under the circumstance.

[3] Following international trade literature convention, home country refers to the origin of multinationals and host country refers to the market where it operates.

Dr. Yat-fai Lam and Dr. Ronald Kwok-ho Chung prepared this case under the supervision of Dr. Clement Yuk-pang Wong for class discussion. This case is not intended to show effective or ineffective handling of decision or business processes. The authors might have disguised certain information to protect confidentiality. Cases are written in past tense, this is not meant to imply that all practices, organizations, people, places or fact mentioned in the case no longer occur, exist or apply.

Ref. 19/640C

Last edited: 11 May 2020

meant additional ongoing compliance costs and effort in the forms of paperwork and manpower. Beyond that, there was an implicitly cost of loss of actual and potential business opportunities arising from having to compromise service quality to its clients due to compliance, such as the inconvenience, delays, and limitation on the scope of services to certain clients.

The risks of non-compliance had been highlighted by disciplinary actions taken by the HKMA against four banks with operations in Hong Kong, three of which were, in fact, multinational banks. Indeed, to avoid a severely escalated cost of compliance and the risk of disciplinary actions, a number of GCBC's competitors had taken a "de-risking" approach by not serving certain segments of the market.

While there were certainly heightened risks, the CEO certainly understood that with risks came opportunities. With many of GCBC's competitors adopting the "de-risking" strategy, perhaps they had left a market niche with unsatisfied client needs.

The CEO decided to call a meeting with the CFO, the COO, the Chief Information and Systems Officer and the Chief Compliance Officer to get an in-depth understanding of HKMA's AML guidelines and assess the costs and the benefits of various action plans.

What was Money Laundering?

Money laundering was the process where money obtained through criminal activities was moved through the financial system so as to disguise its criminal source and the identity of the criminals, giving the money an appearance of legitimacy.

Examples of criminal activities giving rise to illegal funds include financial frauds (such as fraudulent insurance claim, tax evasion and cyber-crime), drug trafficking, smuggling, human trafficking and prostitution, corruption, organized crime, and terrorism.[4] In Hong Kong, proceeds from corruption, tax evasion and smuggling were the key areas of concern.

Money laundering was achieved through a three-stage process:

- Placement, i.e., placing illegitimate proceeds in the financial system, e.g., depositing illegitimate funds into bank accounts;
- Layering, i.e., making it difficult to detect and uncover a laundering activity, e.g., instead of a large deposit which made the laundering easy to detect, small, multiple deposits were made;
- Integration, i.e., placing the laundered proceeds back under the control of its original owner.

The Legislative Background

Money laundering is clearly a global problem that requires global cooperation between international, governmental and private sector bodies. According to the United Nations Office on Drugs and Crime (UNODC), the estimated amount of money laundered globally in one year was "2 to 5% of global GDP".[5] With increasingly interconnected global payment and banking systems, money laundering activities are increasingly difficult to tackle by regulators. As a

[4] https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf
[5] https://www.unodc.org/unodc/en/money-laundering/globalization.html

result, international agencies dedicated to anti-money laundering have been set up to foster international cooperation in clamping down money laundering and, hopefully, illegal activities.

The Financial Action Task Force (FATF) was established at the G7 Summit in Paris in 1989 to develop global standards for anti-money laundering[6] (AML). These global standards, also called the FATF Recommendations, were a comprehensive set of AML measures that the FATF recommended to all countries. Since then, the FATF had expanded to include 37 countries and territories and two regional organizations. Hong Kong is not only a member country of FATF, but was also one of the founding members of the Asia/Pacific Group on Money Laundering, a regional body established in 1997.

The Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance[7]

In 2008, the FATF conducted a comprehensive assessment of the level of compliance of Hong Kong's AML policies and implementations and compared them with the FATF recommendations. It identified a few deficiencies during its assessment including, among others, the lack of statutory backing for the know-your-customer and record-keeping requirements.

The Hong Kong SAR Government embarked on a legislative process to mitigate the shortcomings identified in the FATF assessment the following year. This legislative process resulted in the first ordinance in Hong Kong that established regulatory standards and expectations for the AML compliance programs in designated financial institutions.[8]

The Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance[9] (AMLO) became effective in Hong Kong in April 2012. The ordinance specified the AML regulators and their regulatory duties for certain financial sectors and established a number of requirements that designated financial institutions had to comply with through their AML compliance programs.

The AML Regulator for the Banking Industry[10]

Under the AMLO, the Hong Kong Monetary Authority (HKMA) became the AML regulator that supervised banks' AML compliance programs. In addition to assigning policy and supervision authorities to the HKMA, the AMLO also granted the HKMA the authority to investigate banks' potential violation of the ordinance and to take disciplinary actions against them, subject to the judgment of the HKMA's AML disciplinary committee.

Banks' Compliance of the AMLO

A bank had to establish its AML procedures to comply with the Schedule 2 of the AMLO, especially the following sections from an operation's perspective[11]:

Section 3	When customer due diligence measures must be carried out
Section 4	Simplified customer due diligence

[6] For the sake of brevity, in this case study, the term "money laundering" means "money laundering and terrorist financing."

[7] This ordinance was enhanced and renamed to "Anti-Money Laundering and Counter-Terrorist Financing Ordinance," effective March 2019.

[8] These designated financial institutions include banks, securities firms, insurance companies offering longer term insurance services, remittance agencies, and money changers.

[9] Legislative Council, "Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance," 29 June 2011, https://www.legco.gov.hk/yr10-11/english/ord/ord015-11-e.pdf, accessed 30 April 2019.

[10] The other three AML financial regulators in Hong Kong were the Securities and Futures Commission, the Insurance Authority, and the Custom and Excise Department.

[11] Section 1 is Interpretation, Section 2 describes customer due diligence measures, and Section 8 are additions to requirements in sections 3 and 5, and are, therefore, left out in this list.

Section 5	Duty to continuously monitor business relationships
Section 6	Provisions relating to pre-existing customers
Section 7	Provisions relating to pre-existing respondent banks
Section 9	Special requirements when customer is not physically present for identification purposes
Section 10	Special requirements when customer is politically exposed person
Section 11	Special requirements for insurance policies
Section 12	Special requirements for wire transfers
Section 13	Special requirements for remittance transactions
Section 14	Special requirements for correspondent banking relationships
Section 15	Special requirements in other high-risk situations

Customer Due Diligence

Customer due diligence (CDD) was the most critical of the requirements in the AMLO. Under the CDD process, a bank had to (1) identify the official name of a customer using appropriate instruments, e.g., an application form or image of an identity document; (2) verify the customer's identity using information from independent and reliable sources, e.g., original identity document or government registry; (3) obtain the objective of the business relationship with the bank unless the objective was obvious; (4) check the customer name against the records in a watch list; and (5) conduct an assessment of the money laundering risk of the customer.

When there was a beneficial owner who might benefit from the customer's banking activities, the bank also had to identify, verify, and assess that beneficial owner. If any beneficial owner was classified as higher risk, the customer would also be classified as higher risk.

To accept a higher-risk customer, a bank had to conduct an enhanced CDD to collect further information in order to ascertain that the customer was unlikely to be connected to money laundering activities. In general, a bank could only open an account for a lower-risk customer or a higher-risk customer who was unlikely to engage in money laundering activities. Senior management approval was needed for account opening of customers with high money laundering risk.

A bank needed to identify the beneficial owners of a corporate customer including its major shareholders, directors, and account signatories and, in the event that a major shareholder is a corporation, conduct CDD on major corporate shareholders that appeared in different layers of shareholding structure of the corporate customer.

Politically Exposed Person

A political exposed person (PEP) was an entity entrusted with a prominent public function, such as senior politician, judicial official, or senior officer of a state-owned corporation. By default, a PEP was classified as a higher-risk customer because his office and position might render the PEP vulnerable to corruption. In the same vein, any entity that had a close relationship with a PEP was also considered a PEP.

As with other higher-risk customers, PEPs were subject to the enhanced CDD and senior management approval before account opening.

Continuous Monitoring

After opening an account for a customer, a bank needed to continuously monitor the background and transactions of the customer. If the bank believed that the customer's CDD information was outdated or observed any suspicious transactions connected to the customer, it had to conduct CDD on the customer again.

Wire Transfer

The AMLO put in place specific requirements for wire transfer. For an outgoing wire transfer transaction, a bank had to include in the transfer instructions the legal name of the customer who initiated the transaction.

Response by Banks

De-risking

In an effort to reduce money laundering risk, some banks resorted to a risk avoidance strategy called "de-risking" [12] whereby they applied overly stringent CDD measures that were disproportional to the money laundering risk customers might pose, and, in many cases, denied banking services to these customers. For example, some banks put in place a battery of stringent conditions in their account opening procedures, such as:

- Requiring all directors and beneficial owners of a company, including those incorporated outside Hong Kong, to be present at the account opening.
- Mandating that all documents of a company, including a company incorporated outside Hong Kong, be certified by a qualified certifier in Hong Kong.
- Requesting a start-up to provide its track record, business plan, and revenue projections at the same level of detail as an established company.
- Requiring a Hong Kong business registration certificate and office address of a company, including companies without the need for physical operations in Hong Kong, e.g., online shops.
- Requiring voluminous or detailed evidence to demonstrate a customer's source of wealth, sometimes going back decades.
- Considering other factors in addition to money laundering risk, such as sales turnover, in approving account opening applications.

The trend of de-risking gained momentum among banks after HKMA took actions against some banks. As a result of de-risking, many small and medium enterprises experienced difficulties and unnecessary delays in opening their bank accounts. Consequently, the AMLO had caused the side effect of reducing the efficiency of the banking system.

To contain de-risking and alleviate its side effect, the HKMA encouraged banks to adopt a "risk-based approach" [13] under which the AML measures applied to a customer were proportional to the level of money laundering risk it posed to the bank. However, the risk-based approach was no silver bullet because it involved applying subjective judgment to determine the risk and the corresponding measures. The HKMA did not acknowledge whether the bank could use this risk-based approach as a valid reason to justify deficiencies in its AML compliance program.

In the meantime, since there were no unified and objective metrics in the industry to measure money laundering risk, some banks would cite money laundering risk as a pretext to deny lower-profit margin customers' access to banking services.

[12] HKMA, "De-risking and Financial Inclusion", 8 September 2016, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160908e1.pdf, accessed 30 April 2019.

[13] HKMA, "FATF Risk-Based Approach Guidance for the Banking Sector and Money Laundering and Terrorist Financing Risk Assessment," 19 December 2014, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141219e1.pdf, accessed 30 April 2019.

Violations of the AMLO by Four Banks

Since the AMLO came into effect, the HKMA had been conducting on-site examinations of the AML compliance programs at selected banks in Hong Kong. If it identified material improper practices, it would pass the case to the HKMA's AML investigation team to conduct a comprehensive investigation into the potential violations of the AMLO.

As of the end of 2018, the HKMA had taken disciplinary actions under the AMLO against four banks, namely, State Bank of India, Hong Kong Branch (SBI), Coutts & Co. AG, Hong Kong Branch (Coutts), Shanghai Commercial Bank Limited (SHCB), and JPMorgan Chase Bank, National Association, Hong Kong Branch (JPMC), for their failures to comply with the ordinance, resulting in a total pecuniary penalty of HKD32mn.

When deliberating about disciplinary actions against these four banks, the HKMA had given serious consideration to (1) their willingness to cooperate with the investigation, and (2) the objective of sending a clear message to the banking industry about the importance of combating money laundering.

State Bank of India, Hong Kong Branch

On 31 July 2015, the HKMA reprimanded and fined SBI.[14]

The AML Procedures

From April 2012 to November 2013, SBI largely adopted the HKMA's AML guideline as the bank's AML policies and procedures, with only minor modifications adapted to its institutional practices. However, SBI did not establish any detailed procedures to comply with several major AML control areas until December 2013, such as the CDD measures, PEPs, transaction monitoring, and higher money laundering risk situations.

The CDD Procedures

SBI neither took measure to identify the beneficial owners of 28 corporate customers, nor carried out adequate measures to verify the identities of the beneficial owners in the account opening process. In 22 accounts, SBI did not identify the beneficial owners and did not acquire information from independent and reliable source to verify the beneficial owners. In 17 accounts, SBI did not look into the intermediate layers of companies in their multiple layers of ownership structure in order to trace the ultimate beneficial owners of the customers.

In addition, during the period from April 2012 to December 2012, SBI failed to conduct screening against its internal PEP database for

- all customers and their beneficial owners on a periodic basis, and
- customers' beneficial owners before establishing business relationships with the bank.

Finally, SBI did not periodically review and update the money laundering risk level of its customers until February 2013. Customers who were classified as higher risk were not subject to periodic CDD review until February 2013.

[14] HKMA, "Monetary Authority takes disciplinary action against State Bank of India, Hong Kong Branch for contraventions of specified provisions under the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance," 31 July 2015, https://www.hkma.gov.hk/eng/key-information/press-releases/2015/20150731-5.shtml, accessed 30 April 2019.

Transaction Monitoring

SBI could not identify suspicious transactions from four system generated reports. In addition, SBI could not provide any evidence that it had put in place any transaction monitoring system before December 2013.

Contraventions of the AMLO

The HKMA concluded that SBI had contravened sections 3(1), 5(1), 19(1), and 19(3) of Schedule 2 of the AMLO from April 2012 to November 2016.

Disciplinary Actions

The HKMA ordered SBI to:

(a) Pay a pecuniary penalty of HKD7.5mn.
(b) Submit an independent assessment report, detailing whether the corrective actions taken were sufficient and effective to address the deficiencies identified by the HKMA.

Additional Regulatory Considerations

When deciding on the disciplinary actions, the HKMA had considered the following factors, in addition to the two common regulatory considerations:

(a) SBI replaced the Chief Executive in October 2013.

(b) SBI's external consultant confirmed that no problematic accounts and/or suspicious transactions were identified.

(c) SBI had implemented a corrective action plan recommended by an external consultant and had taken very positive and intensive actions to enhance its AML compliance program to address the deficiencies identified.

(d) SBI had engaged an external consultant to conduct extensive review and an audit firm to audit the AML compliance program on an ongoing basis.

(e) SBI had no previous disciplinary record in relation to the AMLO.

Coutts & Co. AG, Hong Kong Branch

On 11 April 2017, the HKMA reprimanded and fined Coutts[15] after the HKMA had completed an AML compliance investigation of the bank's private banking services.

Politically Exposed Persons

Coutts did not seek senior management's approval of its business relationship with nine PEPs. In five scenarios, Coutts had received earlier PEP alerts but did not follow up promptly. In other four scenarios, Coutts did not qualify four customers as PEPs even though their information had been available either on a commercially available database or from publicly available sources. As a result, it did not classify these four PEPs as higher-risk customers for several years. Thus, there were delays from 4 to 34 months in the nine scenarios before the bank finally took appropriate actions, such as obtaining approval for new accounts from senior management or terminating existing accounts.

Other Higher-Risk and/or Complex Customers

Coutts did not obtain approval from the senior management for continuing its business relationship with a corporate customer with a doubtful beneficial owner. The beneficial owner

[15] HKMA, "The Monetary Authority reprimands and fines Coutts & Co AG, Hong Kong Branch for contraventions of the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance," 11 April 2017, https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170411-4.shtml, accessed 30 April 2019.

was a charitable foundation closely connected to a higher-risk country, and the parties that ultimately controlled the charitable foundation were not clarified.

Coutts did not take sufficient measures to discern the ownership and control structure of a corporate customer where legal persons and trust were involved in the corporate structure of the customer. In this scenario, the control structure of the corporate customer actually comprised five intermediate layers, multiple companies, multiple jurisdictions, and a trust.

Contraventions of the AMLO

The HKMA concluded that Coutts had contravened sections 3(1), 10(2), 15, 19(1), and 19(3) of Schedule 2 of the AMLO from April 2012 to June 2015.

Disciplinary Actions

The HKMA ordered Coutts to pay a pecuniary penalty of HKD7mn.

Additional Regulatory Considerations

When deciding the disciplinary actions, the HKMA had taken into account the following factors, in addition to the two common regulatory considerations:

(a) Coutts had engaged an external consultant to conduct extensive review of its policies and procedures and remediation of customer files.

(b) Coutts had implemented a corrective action plan recommended by an external consultant and had taken very positive and intensive actions to enhance its AML compliance program to address deficiencies identified.

Shanghai Commercial Bank Limited

On 17 August 2018, the HKMA reprimanded and fined SHCB[16] after it had completed an investigation of the bank's AML compliance program.

Transaction Monitoring

SHCB relied on a transaction monitoring system to screen suspicious transactions. From July 2014 to June 2016, the transaction monitoring system generated a total of 24,225 alerts. After the business units had reviewed the alerts and supplemented further information, the Compliance Department identified 394 alerts involving 321 customers for further investigations. Of these 394 alerts, transactions in 40 alerts involving 33 customers were identified to be complex, unusually large in amount, and unusual in transaction pattern, or had no apparent economic purposes behind the transactions. Nevertheless, SHCB did not adequately examine the background behind and purposes of these transactions and did not record the findings in writing. For 11 of the 33 customers, the relevant transactions took place between September 2014 and March 2016, but SHCB did not submit suspicious transaction reports to the Joint Financial Intelligence Unit (JFIU) until November 2016, after the HKMA's investigation team had examined the alerts.

In one alert, funds were transferred through a number of individual and corporate accounts owned by the same customer and ultimately deposited into a company's account for alleged investment purposes. However, the bank neither enquired why the fund transfers were structured in such a complicated way, nor examined the background and/or purposes of the transaction, and did not record the findings in writing.

[16] HKMA, "The Monetary Authority reprimands and fines Shanghai Commercial Bank Limited for contraventions of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance," 17 August 2018, https://www.hkma.gov.hk/eng/key-information/press-releases/2018/20180817-5.shtml, accessed 30 April 2019.

In a second alert, an individual customer received a single payment of over HKD75mn from a corporate counterparty. The business unit explained that the amount was a loan granted by the counterparty for business purposes. Despite the significant amount of the alleged loan and its business nature, the bank did not enquire why the fund was deposited into the customer's personal account instead of his company's corporate account. In fact, SHCB had established in its internal policies and procedures that "using personal accounts to handle commercial transactions of companies" was one of the red flags of tax evasion.

In a third alert, an individual customer received a check exceeding HKD20mn from another individual. The bank only documented the name of the counterparty in the internal records. There was no examination of the background of the counterparty and his business relationship with the customer, as well as the purposes behind the transaction.

The CDD for Customers Connected to Suspicious Transactions

The SHCB did not carry out the CDD for certain customers who were connected to suspicious transactions identified by the transaction monitoring system from July 2012 to June 2017.

In one situation, the personal account of a customer was used as a temporary repository for funds, which was one of the common suspicious indicators of money laundering established by the JFIU. However, even though the customer's explanation of the transactions was implausible and/or inconsistent with SHCB's knowledge of the customer's background, the bank did not conduct the CDD to update the customer information.

Contraventions of the AMLO

The HKMA concluded that SHCB had contravened sections 5(1) and 19(3) of Schedule 2 of the AMLO from July 2014 to June 2016, and section 6(1) of Schedule 2 of the AMLO from July 2012 to June 2017.

Disciplinary Actions

The HKMA ordered SHCB to:

(a) Pay a pecuniary penalty of HKD5.0mn.

(b) Submit an independent assessment report, detailing whether the corrective actions SHCB took were sufficient and effective to address the deficiencies it identified.

Additional Regulatory Considerations

When deciding the disciplinary actions, the HKMA had taken into account the following factors, in addition to the two common regulatory considerations:

(a) SHCB had started to implement corrective actions to enhance its AML compliance program.

(b) SHCB had no previous disciplinary record in relation to the AMLO.

JPMorgan Chase Bank, National Association, Hong Kong Branch

On 28 December 2018, the HKMA reprimanded and fined JPMC,[17] after it had completed an investigation of the AML compliance program of JPMC's private banking services.

[17] HKMA, "The Monetary Authority reprimands and fines JPMorgan Chase Bank, National Association, Hong Kong Branch for contraventions of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance," 28 December 2018, https://www.hkma.gov.hk/eng/key-information/press-releases/2018/20181228-3.shtml, accessed 30 April 2019.

The CDD Procedures

JPMC had conducted a gap analysis between its CDD procedures (JPCDD) and the AMLO before the enactment of the AMLO. After the gap analysis, JPMC updated its CDD procedures. However, a number of deficiencies in its CDD procedures remained:

(a) JPCDD procedures did not require a certificate of incumbency or equivalent official document to be collected in order to verify the existence of a corporate customer.

(b) JPCDD procedures only required verification of beneficial owners for higher-risk customers. The requirement was not mandated for lower-risk customers.

(c) For a group of corporate customers with substantial shareholding relationships, the JPCDD procedures allowed the periodic CDD review of the group of corporate customers to be conducted on a sampling basis. That meant that if the periodic JPCDD review had been completed on one group member, with the documents, data, and information relating to that particular group member being up-to-date and relevant, then it deemed the regular JPCDD reviews of all members within the same relationship group to be completed.

The CDD Samples

(a) JPMC did not conduct a periodic CDD review on 259 of 495 higher-risk corporate customers. These corporate customers belonged to some relationship groups in which at least one of the member customers had been subject to the periodic CDD review.

(b) JPMC did not (1) collect identification document from, and/or (2) ascertain the purpose and/or intended use of the account by certain customers.

(c) JPMC did not conduct enhanced CDD on a few customers who were qualified as PEPs under the AMLO.

Coded Account Names

JPMC used alphanumeric codes as account names for a select group of customers. It then used the account name in code format, instead of the genuine customer name, in all banking operations in relation to customers in order to hide the customers' identities. The use of coded account names prevented the genuine customer names from being exhibited in the bank's computer systems and documents, thus providing extra privacy protection to selected customers. When JPMC carried out outgoing wire transfers from code-named accounts, the corresponding SWIFT messages contained the coded account name as the originator. In other words, it became impossible to identify the customer simply from the SWIFT messages.

Contraventions of the AMLO

The HKMA concluded that JPMC had contravened sections 3(1), 5(1), 12(5), 19(1), 19(2), and 19(3) of Schedule 2 of the AMLO from April 2012 to February 2014.

Disciplinary Actions

The HKMA ordered the JPMC to

(a) Pay a pecuniary penalty of HKD12.5mn.

(b) Submit an independent assessment report, detailing whether the corrective actions it took were sufficient and effective to address the deficiencies identified by the HKMA.

Additional Regulatory Considerations

When deciding the disciplinary actions, the HKMA had taken into account the following factors, in additional to the two common regulatory considerations:

(a) The level of severity of the contraventions under the Schedule 2 to the AMLO, in particular with the establishment and maintenance of effective procedures.

(b) JPMC had voluntarily reported certain deficiencies and had taken comprehensive action to address the deficiencies identified.

(c) JPMC had no previous disciplinary record in relation to the AMLO.

Challenges Facing the Banking Industry, Regulators, and Society

The AMLO had force banks to expend more resources to combat money laundering activities. The bank regulator observed that banks and money launderers also responded to the ordinance in other ways that had implications for the banking industry.

Since the enhanced CDD procedures were costly to implement, banks tended to conduct such procedures only on higher-profit margin customers. Consequently, although designed to control money laundering risk, the enhanced CDD procedures were used instead by some banks as a tool to cherry-pick wealthy customers. What could be done so that legitimate, lower-profit customers would not be denied banking services just because of their money laundering risk profile?

To the extent that countries adopted AML standards at different pace, some banks, since the introduction of the AMLO, have engaged in intercountry regulatory arbitrage in which international banking groups relocated their operations from countries with more stringent AML regimes to those with less.

In addition, while the AMLO had made it more costly for criminals to use the banking system as a conduit for money laundering, no similar regulatory oversight existed for nonbank money lenders. Thus, it was conceivable that money launderers would shift their activities from banks to nonbank money lenders. Would this render the AMLO ineffective in combating money laundering?

The Chief Executive of GCBC wondered how the bank should respond to money laundering risks and the requirements of AMLO. Should the bank beef up its AML practices, or risk following the fate of the four disciplined banks? What is the optimal amount of resources to be committed to AML? Should it set up non-bank money lending subsidiaries? Should it move its operations to other countries with less stringent AML regulations? Looking at the practice of “de-risking” among its peers, the Chief Executive also wondered whether the AMLO was well designed to combat money laundering activities, and whether the ordinance’s social benefits outweighed its social costs.

APPENDIX – SELECTED SECTIONS OF SCHEDULE 2, THE AMLO

3. When customer due diligence measures must be carried out

(1) Subject to section 4 of this Schedule, a financial institution must carry out customer due diligence measures in relation to a customer in the following circumstances:

(a) subject to subsection (2), before establishing a business relationship with the customer.
(b) before carrying out for the customer an occasional transaction involving an amount equal to or above HKD120,000 or an equivalent amount in any other currency, whether the transaction is carried out in a single operation or in several operations that appear to the financial institution to be linked.
(c) despite paragraph (b), before carrying out for the customer an occasional transaction that is a wire transfer involving an amount equal to or above HKD8,000 or an equivalent amount in any other currency, whether the transaction is carried out in a single operation or in several operations that appear to the financial institution to be linked.
(d) when the financial institution suspects that the customer or the customer's account is involved in money laundering or terrorist financing.
(e) when the financial institution doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

5. Duty to continuously monitor business relationships

(1) A financial institution must continuously monitor its business relationship with a customer by:

(a) reviewing from time to time documents, data and information relating to the customer that have been obtained by the financial institution for the purpose of complying with the requirements imposed under this Part to ensure that they are up-to-date and relevant.
(b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the financial institution's knowledge of the customer and the customer's business and risk profile, and with its knowledge of the source of the customer's funds.
(c) identifying transactions that—
    (i) are complex, unusually large in amount or of an unusual pattern.
    (ii) have no apparent economic or lawful purpose, and examining the background and purposes of those transactions and setting out its findings in writing.

6. Provisions relating to pre-existing customers

(1) In relation to a pre-existing customer who is not a customer to whom section 7 of this Schedule applies, a financial institution must, in addition to the situations specified in section 3(1)(d) and (e) of this Schedule, carry out the customer due diligence measures when—

(a) a transaction takes place with regard to the customer that—

(i) is, by virtue of the amount or nature of the transaction, unusual or suspicious. or

(ii) is not consistent with the financial institution's knowledge of the customer or the customer's business or risk profile, or with its knowledge of the source of the customer's funds. or

(b) a material change occurs in the way in which the customer's account is operated.

10. Special requirements when customer is politically exposed person

(2) If a financial institution comes to know, from publicly known information or information in its possession, that an existing customer or a beneficial owner of an existing customer is a politically exposed person or has become a politically exposed person, it must not continue its business relationship with the customer unless it

(a) has obtained approval from its senior management.

(b) has taken reasonable measures to establish the customer's or beneficial owner's source of wealth and the source of the funds that are involved in the business relationship.

12. Special requirements for wire transfers

(3) Before carrying out a wire transfer, a financial institution that is an ordering institution must record:

(a) the originator's name.

(b) the number of the originator's account maintained with the financial institution and from which the money for the wire transfer is paid or, in the absence of such an account, a unique reference number assigned to the wire transfer by the financial institution.

(c) the originator's address or, in the absence of an address, the originator's customer identification number or identification document number or, if the originator is an individual, the originator's date and place of birth.

(5) Subject to subsections (6) and (7), a financial institution that is an ordering institution must include in the message or payment form accompanying the wire transfer the information recorded under subsection (3) in relation to the transfer.

15. Special requirements in other high risk situations

A financial institution must, in a situation specified by the relevant authority in a notice in writing given to the financial institution and in any other situation that by its nature may present a high risk of money laundering or terrorist financing:

(a) where a business relationship is to be established

(i) obtain approval from its senior management to establish the business relationship.

(ii) Either

(A) take reasonable measures to establish the relevant customer's or beneficial owner's source of wealth and the source of the funds that will be involved in the business relationship, or

(B) take additional measures to mitigate the risk of money laundering or terrorist financing involved.

(b) where a business relationship has been established:

(i) obtain approval from its senior management to continue the business relationship.

(ii) if there is a beneficial owner in relation to the relevant customer, take reasonable measures to verify the beneficial owner's identity so that the financial institution is satisfied that it knows who the beneficial owner is.

(iii) either

(A) take reasonable measures to establish the relevant customer's or beneficial owner's source of wealth and the source of the funds that are involved in the business relationship, or

(B) take additional measures to mitigate the risk of money laundering or terrorist financing involved, or

(C) where an occasional transaction is to be carried out, take additional measures to mitigate the risk of money laundering or terrorist financing involved.

19. Financial institutions to establish procedures

(1) A financial institution must establish and maintain effective procedures for determining whether a customer or a beneficial owner of a customer is a politically exposed person.

(2) A financial institution that carries out wire transfers must establish and maintain effective procedures for identifying and handling wire transfers in relation to which section 12(5) of this Schedule has not been complied with.

(3) A financial institution must, in respect of each kind of customer, business relationship, product and transaction, establish and maintain effective procedures not inconsistent with this Ordinance for the purpose of carrying out its duties under sections 3, 4, 5, 9, 10 and 15 of this Schedule.