International
Comparative
Legal Guides

Anti-Money Laundering

2024

Seventh Edition

Contributing Editors:
Stephanie Brooker & M. Kendall Day
Gibson, Dunn & Crutcher LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Singapore


Gary Low


Terence Tan

Drew & Napier LLC

1 The Crime of Money Laundering and Criminal Enforcement

1.1 What is the legal authority to prosecute money laundering at the national level?

The Attorney-General in his role as the Public Prosecutor ("**PP**") prosecutes money laundering ("**ML**") offences in Singapore.

1.2 What must be proven by the government to establish money laundering as a criminal offence? What money laundering predicate offences are included? Is tax evasion a predicate offence for money laundering?

The primary legislation targeting ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("**CDSA**").[1]

The main ML offences are contained in Sections 50, 51, 53, 54 and 55 of the CDSA. Although the CDSA does not specifically define ML, it criminalises the dealing in property that represents, in whole or in part, and directly or indirectly, the benefits of drug dealing or criminal conduct ("**Criminal Benefits**").

Sections 53(1) and 54(1) of the CDSA criminalise "primary" ML (i.e. laundering the accused person's own Criminal Benefits). These provisions criminalise acquiring, possessing, using, concealing or transferring property representing the accused person's Criminal Benefits. The PP must prove, in relation to such property, that the accused:

(a) concealed or disguised such property;
(b) converted, transferred or removed such property from the jurisdiction; or
(c) acquired, possessed or used such property.

Sections 53(2) and 54(2) of the CDSA criminalise "secondary" ML (i.e. laundering someone else's Criminal Benefits). These provisions criminalise concealing, disguising, converting, transferring or removing from the jurisdiction someone else's Criminal Benefits. The PP must prove in relation to such property that:

(a) the accused concealed, disguised, converted, transferred or removed such property from the jurisdiction; and
(b) that the accused did so knowing or having reasonable grounds to believe that the property was someone else's Criminal Benefit.

Section 55 of the CDSA criminalises the possession or use of any property that may reasonably be suspected to be Criminal Benefits, if the accused is unable to satisfactorily account for how he came by the property.

Sections 50 and 51 of the CDSA criminalise assisting another person to retain their Criminal Benefits. Under both Sections, the PP must prove that the accused had entered into or was otherwise concerned in an arrangement, and that the accused did so while knowing or having reasonable grounds to believe that the arrangement would:

(a) facilitate the retention or control of the other person's Criminal Benefits by or on behalf of the other person, whether by concealment, removal from jurisdiction, transfer to nominees, or otherwise;
(b) use the other person's Criminal Benefits to secure funds that are placed at that other person's disposal, directly or indirectly, or use the other person's Criminal Benefits for the other person's benefit to acquire property by way of investment or otherwise; and
(c) the other person is a person who engages in or has engaged in drug dealing/criminal conduct, or who has benefitted from drug dealing/criminal conduct.

Predicate offences

The CDSA prescribes a wide range of predicate offences. The provisions criminalising ML refer to benefits of "*drug dealing*" or "*criminal conduct*".

The term "*drug dealing*" refers to the offences specified in the First Schedule of the CDSA as well as abetment of such offences, and includes a "*foreign drug dealing offence*", which is an "*offence against a corresponding law*", and which would have constituted a drug-dealing offence if it occurred in Singapore.

The term "*criminal conduct*" refers to any act constituting either a "*serious offence*" or a "*foreign serious offence*". A serious offence is an offence specified in the Second Schedule of the CDSA, and a foreign serious offence is an offence against the law of a foreign country, including conduct that would have constituted a serious offence if it had occurred in Singapore. This includes bribery, cheating, criminal breach of trust, forgery, theft and robbery, among other things.

Tax evasion as a predicate offence for money laundering

Yes, tax evasion is a predicate offence for money laundering in Singapore.

Offences relating to tax evasion under the Goods and Services Act 1993 and Income Tax Act 1947 are listed in the Second Schedule of the CDSA as serious offences. An offence against the law of a foreign country that would have constituted tax evasion if it had occurred in Singapore would also constitute a foreign serious offence (see Section 2(1) CDSA).

1.3 Is there extraterritorial jurisdiction for the crime of money laundering? Is money laundering of the proceeds of foreign crimes punishable?

Yes. The CDSA applies to ML offences in respect of property representing benefits of certain categories of foreign crimes, if those offences consist of or involve conduct that would have constituted offences in Singapore under the First Schedule or Second Schedule of the CDSA.

The CDSA also applies to any property, whether situated in Singapore or elsewhere (see Section 4(5) CDSA).

1.4 Which government authorities are responsible for investigating and prosecuting money laundering criminal offences?

The primary investigative agency for ML offences is the Commercial Affairs Department ("**CAD**") of the Singapore Police Force ("**SPF**"). Officers of the Central Narcotics Bureau and the Corrupt Practices Investigation Bureau are also involved in investigating certain kinds of ML offences.

ML offences are prosecuted by the PP, who is authorised to assign his prosecutorial duties to Deputy Public Prosecutors and Assistant Public Prosecutors, who carry out such PP functions.

1.5 Is there corporate criminal liability or only liability for natural persons?

There is both corporate criminal liability and liability for natural persons.

1.6 What are the maximum penalties applicable to individuals and legal entities convicted of money laundering?

The maximum penalty under Sections 50, 51, 53 and 54 of the CDSA is:

- for an individual, a fine not exceeding S$500,000 or imprisonment not exceeding 10 years, or both; and
- for a non-individual, a fine not exceeding S$1 million or twice the value of the benefits of the drug dealing/criminal conduct in respect of which the offence was committed, whichever is higher.

The maximum penalty under Section 55 of the CDSA is:

- for an individual, a fine not exceeding S$150,000 or imprisonment not exceeding three years, or both; and
- for a non-individual, a fine not exceeding S$300,000.

1.7 What is the statute of limitations for money laundering crimes?

There is no statute of limitations for the prosecution of ML crimes, or for the prosecution of criminal offences in general. Nevertheless, where there has been an inordinate delay in prosecution, this may be a factor considered by the court in sentencing.

1.8 Is enforcement only at national level? Are there parallel state or provincial criminal offences?

Yes, enforcement is only at national level. There is no "state" or "provincial" criminal legislation, as there are no states or provinces in Singapore.

1.9 Are there related forfeiture/confiscation authorities? What property is subject to confiscation? Under what circumstances can there be confiscation against funds or property if there has been no criminal conviction, i.e., non-criminal confiscation or civil forfeiture?

The PP may apply to court for property to be confiscated under the CDSA and the Organised Crime Act 2015 ("**OCA**").[2] While investigative agencies may seize property or freeze bank accounts, confiscation or forfeiture is done by court order.

When a defendant is convicted of one or more predicate offences listed in the CDSA, the PP may apply to the court for a confiscation order. Benefits derived by the defendant from his drug dealing or criminal conduct will be subject to a confiscation order if the court is satisfied that such benefits have been so derived (Sections 6 and 7 CDSA).

Where there has been no criminal conviction, material or financial gains from organised crime activity can also be confiscated under the OCA. Such a confiscation order under the OCA does not require that the organised crime activity be the subject of any criminal proceedings (Section 51 OCA). The discontinuance or acquittal of the defendant in any such criminal proceedings would not impact the confiscation order (Section 53 OCA). The PP may apply for a confiscation order under the OCA, and the court will make a confiscation order if the court is satisfied, on a balance of probabilities, that the person has carried out an organised crime activity within the defined statutory period and has derived benefits from the organised crime activity (Section 61 OCA).

"*Organised crime activity*" refers to any activity carried out by a person in (or outside) Singapore amounting to a serious offence specified in the Schedule to the OCA (which includes Sections 50, 51, 53 and 54 CDSA) and is carried out at the direction of or in furtherance of the illegal purpose of a group that the person knows or has reasonable grounds to believe is an organised criminal group (Section 48(1)(a)–(b) OCA). Where the activity is carried out by a person outside Singapore, the organised criminal group must be locally linked.

Such "*organised crime activity*" also includes being a member of an organised criminal group, recruiting members for such a group, instructing the commission of offences for such a group, and otherwise supporting or aiding such a group (Section 48(1)(c) OCA read with Part 2 OCA).

1.10 Have banks or other regulated financial institutions or their directors, officers or employees been convicted of money laundering?

Officers and employees of regulated financial institutions ("**FIs**") have previously been convicted of ML offences in Singapore.

In July 2017, Yeo Jiawei, a former wealth planner at BSI Bank Limited, was sentenced to 54 months' imprisonment for ML and cheating in a case related to the probe into Malaysian state fund 1Malaysia Development Berhad ("**1MDB**"). Two other former BSI bankers, Yak Yew Chee and Yvonne Seah Yew Foong, were also sentenced to jail terms of 18 weeks and two weeks, respectively, for forgery and failure to report suspicious transactions connected to the 1MDB case. A former branch manager of Falcon Private Bank, Jens Sturzenegger, was also sentenced to 28 weeks' imprisonment and a S$128,000 fine for failing to report suspicious transactions connected to the same case.

If an FI is convicted of ML offences, it may lose its licence. If the Monetary Authority of Singapore ("**MAS**") is satisfied that a licensed bank is contravening or has contravened any provision of the Monetary Authority of Singapore Act 1970 ("**MAS Act**")

or any direction by MAS under said Act, MAS may by order revoke its bank licence (see Section 20 Banking Act 1970[3] read with Section 27B MAS Act).[4]

There do not appear to be any cases of FIs being convicted of ML offences and losing their licences as a result. However, there are other examples of FIs losing their licences for breach of other Anti-Money Laundering/Countering the Financing of Terrorism ("**AML/CFT**") requirements imposed by MAS. For example, in July 2020, MAS imposed regulatory sanctions on Apical Asset Management Pte Ltd and revoked their Capital Markets Services licence for serious breaches of AML/CFT requirements under MAS Notice SFA04-N02, which exposed the company to the risk of receiving and/or laundering Criminal Benefits. Based on the public information, it does not appear that Apical Asset Management Pte. Ltd. was further prosecuted or convicted of ML offences.

1.11 How are criminal actions resolved or settled if not through the judicial process? Are records of the fact and terms of such settlements public?

Criminal proceedings may be withdrawn or discontinued at the pre-trial stage after negotiations between the Defence and the Prosecution. If the Prosecution agrees, they may withdraw the charges and issue a warning or allow for the offences to be compounded *in lieu* of prosecution.

It would not be accurate to describe this as a settlement, and the reasoning for the Prosecution's exercise of discretion has been kept private and not made available either to the Defence or the public in general.

Deferred Prosecution Agreement ("DPA")

Certain specified criminal actions against a company, partnership or unincorporated association, including those in respect of offences under Sections 50, 51, 53 and 54 of the CDSA, may be resolved through DPAs (Part 7A Criminal Procedure Code 2010 ("**CPC**")).[5]

DPAs are not available to individuals (Section 149D(1) CPC).

A DPA is an agreement entered into between the PP and the company, partnership or unincorporated association under which the PP agrees not to prosecute the alleged offence if the company, partnership or unincorporated association agrees to comply with the requirements imposed on it by the DPA (Sections 149A and 149C CPC). The requirements that a DPA may impose include paying a financial penalty, compensating victims of the alleged offence and disgorging any profits made from the alleged offence (Section 149E(3) CPC).

DPAs are subject to judicial oversight. A DPA only comes into force if the General Division of the High Court approves the DPA and declares that the DPA is in the interest of justice and that its terms are fair, reasonable and proportionate (Section 149F CPC). After such approval, the DPA is published.

1.12 Describe anti-money laundering enforcement priorities or areas of particular focus for enforcement.

AML enforcement priorities are focused on: (a) corporations and professional service providers who become involved with ML and terrorism financing; (b) individuals who act as money mules for overseas organised syndicates (i.e. where an individual is paid to accept money transfers into his bank account and transfer them out again, so as to cover the tracks of illicit funds); and (c) dealers in precious stones and/or precious metals ("**PSM**").

To target corporations and professional service providers, in 2018, penalties for ML offences committed by non-individuals (i.e. entities) were increased in order to strengthen deterrence.

To combat overseas organised syndicates and their ML operations involving money mules, Section 55 of the CDSA was introduced to criminalise the possession or use of any property that may reasonably be suspected to be Criminal Benefits (see question 1.2).

For PSM dealers, a risk-based supervisory and regulatory regime was implemented in 2019 to mitigate ML and terrorism-financing risks in the PSM sector (the Guidelines for Regulated Dealers).[6] The Ministry of Law's Anti-Money Laundering/Countering the Financing of Terrorism Division ("**ACD**") in charge of the regime identified unregistered dealings and compliance with AML/CFT regulations as areas of particular focus for enforcement between October 2019 to March 2021. The ACD also listed regulated dealings via online platforms and higher-risk regulated dealers as enforcement priorities in 2021/2022. At the time of writing, the ACD has not yet published an updated report for 2024.

2 Anti-Money Laundering Regulatory/Administrative Requirements and Enforcement

2.1 What are the legal or administrative authorities for imposing anti-money laundering requirements on financial institutions and other businesses? Please provide the details of such anti-money laundering requirements.

MAS imposes AML requirements on FIs in Singapore.

Other authorities impose AML requirements on non-financial businesses and professions ("**Designated Businesses**"), such as:

- the Gambling Regulatory Authority (for gambling services) (replacing the Casino Regulatory Authority);
- the Accounting and Corporate Regulatory Authority ("**ACRA**") (for corporate service providers, public accountants and accounting entities); and
- the Council for Estate Agencies ("**CEA**") (for estate agents and salespersons).

Details of these requirements can be found in section 3 below.

2.2 Are there any anti-money laundering requirements imposed by self-regulatory organisations or professional associations?

Yes. The Institute of Singapore Chartered Accountants imposes AML requirements on professional accountants, and the Law Society of Singapore imposes AML requirements on law practices and legal practitioners.

2.3 Are self-regulatory organisations or professional associations responsible for anti-money laundering compliance and enforcement against their members?

Yes. For example, legal practitioners and law practices that contravene AML requirements under the Legal Profession Act 1966 (including the Legal Profession (Prevention of Money Laundering and Financing of Terrorism) Rules 2015) may be subject to disciplinary proceedings or regulatory action.

2.4 Are there requirements only at national level?

Yes, see question 1.8.

2.5 Which government agencies/competent authorities are responsible for examination for compliance and enforcement of anti-money laundering requirements? Are the criteria for examination publicly available?

MAS enforces AML requirements under MAS-administered laws and regulations.

Yes, reference can be made to the MAS Enforcement Monograph,[7] which outlines MAS's approach to enforcement and its various AML guidelines.

2.6 Is there a government Financial Intelligence Unit ("FIU") responsible for analysing information reported by financial institutions and businesses subject to anti-money laundering requirements?

Yes, the Suspicious Transaction Reporting Office ("**STRO**") is Singapore's FIU. The STRO receives and analyses suspicious transaction reports ("**STRs**"), cash transaction reports ("**CTRs**") and cash movement reports ("**CMRs**") for physical currency and bearer negotiable instruments ("**CBNIs**"). Information is then disseminated to the relevant enforcement and regulatory agencies where possible offences are detected.

2.7 What is the applicable statute of limitations for competent authorities to bring enforcement actions?

There is no limitation period for enforcement actions.

For information on the responsibilities of Singapore's FIU, see question 2.6.

2.8 What are the maximum penalties for failure to comply with the regulatory/administrative anti-money laundering requirements and what failures are subject to the penalty provisions?

Penalties for failure to comply with AML requirements vary across industries.

Section 16(4) of the Financial Services and Markets Act 2022 ("**FSMA**")[8] stipulates that an FI that fails to comply with any AML direction issued or regulation made by MAS is liable to a fine not exceeding S$1 million, and in the case of a continuing offence, is also subject to a further fine of S$100,000 for every day or part of a day during which the offence continues after conviction.

2.9 What other types of sanction can be imposed on individuals and legal entities besides monetary fines and penalties?

The types of sanctions that can be imposed vary across industries.

For FIs, MAS has power to impose sanctions such as:

- revocation or suspension of licences;
- removal of directors and officers;
- prohibition orders ("**POs**") barring persons from conducting regulated activities or from taking part in management of an FI;
- reprimands; and
- warnings.

2.10 Are the penalties only administrative/civil? Are violations of anti-money laundering obligations also subject to criminal sanctions?

No, violations of AML obligations may also be subject to criminal sanctions.

For example, in relation to FIs, MAS has the power to issue directions to FIs that it considers necessary for the prevention of ML, and failure to comply is a criminal offence (see question 2.8).

Section 174(2) of the FSMA provides that an officer or an individual involved in the management of the FI and in a position to influence the conduct of the FI in relation to the commission of the offence would be guilty of the same offence as the FI if he:

(i) consented or connived, or conspired with others, to effect the commission of the offence;
(ii) was in any other way, whether by act or omission, knowingly concerned in, or party to, the commission of the offence; or
(iii) knew or ought reasonably to have known that the offence by the corporation (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence.

Under Section 7 of the FSMA, MAS will also be able to make POs to bar any persons from carrying out any regulated activities or from holding key roles in any FIs for a period of time, if it is satisfied that these individuals are not fit and proper persons in accordance with the Guidelines on Fit and Proper Criteria.[9] Failure to comply with a PO is similarly a criminal offence (Section 8 FSMA).

2.11 What is the process for assessment and collection of sanctions and appeal of administrative decisions? a) Are all resolutions of penalty actions by competent authorities public? b) Have financial institutions challenged penalty assessments in judicial or administrative proceedings?

In general, the relevant regulatory authority will assess the appropriate sanction(s) to be imposed based on its own internal guidelines and precedents. Judicial review of administrative decisions is possible.

(a) Not all resolutions of "penalty actions" are published, although the facts and circumstances of certain cases may be published by the relevant regulatory authorities (e.g. MAS, ACRA or CEA) at their discretion.
(b) There do not appear to be any reported instances in which FIs have challenged penalty assessments in judicial or administrative proceedings.

3 Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

3.1 What financial institutions and non-financial businesses and professions are subject to anti-money laundering requirements? Describe any differences in the anti-money laundering requirements that each of them are subject to.

FIs subject to AML requirements include:

- banks;
- merchant banks;
- finance companies;

- money changers;
- remittance agents;
- insurers;
- insurance brokers;
- capital markets intermediaries;
- trust companies;
- financial advisers;
- the Central Depository (Pte) Ltd ("**CDP**"); and
- stored value facility holders.

Other Designated Businesses subject to AML requirements include:

- casino operators;
- corporate service providers;
- estate agents and salespersons;
- digital token service providers (also known as Virtual Assets Service Providers ("**VASPs**"));
- payment service providers ("**PSPs**");
- moneylenders;
- pawnbrokers;
- legal practitioners and law practices;
- professional accountants and professional accounting firms (including public accountants and accounting entities); and
- PSM dealers.

In general, the types of AML requirements are similar for FIs and Designated Businesses. Both are required to implement procedures regarding:

- risk assessment and risk mitigation, and applying a risk-based approach;
- customer due diligence ("**CDD**");
- recordkeeping;
- suspicious transaction reporting; and
- other internal policies, procedures, and controls.

The AML requirements vary across sectors. As MAS adopts a risk-based approach, the AML requirements are calibrated according to the degree of risk posed by FIs and Designated Businesses. FIs and Designated Businesses with higher exposure to ML risks would be subject to more AML requirements. More details can be found below.

3.2 Describe the types of payments or money transmission activities that are subject to anti-money laundering requirements, including any exceptions.

The types of payments or money transmission activities subject to AML requirements include:

- account issuance services;
- domestic money transfer services;
- cross-border money transfer services;
- merchant acquisition services;
- e-money issuance services;
- digital payment token ("**DPT**") services; and
- money-changing services.

These PSPs are obliged to register and apply for a PSP licence under the Payment Services Act 2019 ("**PSA**"),[10] and must also meet the AML/CFT requirements under MAS Notice PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism.[11]

Services relating to limited purpose DPTs and limited purpose e-money are excluded from requirements imposed under the PSA (see Part 2 of the First Schedule of the PSA).

3.3 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry? Describe the types of cryptocurrency-related businesses and activities that are subject to those requirements.

Cryptocurrency companies (also known as DPT service providers) are obliged to register and apply for a PSP licence under the PSA. Cryptocurrency companies must also meet the AML/CFT requirements under MAS Notice PSN02 Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service.[12]

The types of cryptocurrency-related businesses and activities subject to AML requirements include the following DPT services:

- dealing in DPTs;
- facilitating the exchange of DPTs, where the service providers may not themselves possess DPTs (also known as VASPs);
- transferring, or arranging for the transfer of, DPTs (DPT transfer service); and
- safekeeping and administration of DPTs or instruments enabling control over DPTs (custodial wallet service).

3.4 To what extent do anti-money laundering requirements apply to non-fungible tokens ("NFTs")?

NFTs are not specifically regulated under Singapore law. Nevertheless, existing AML requirements may apply to NFTs depending on their underlying characteristics.

In a written reply to a parliamentary question on the regulation of NFTs (15 February 2022), Mr Tharman Shanmugaratnam, Senior Minister and Minister in charge of MAS, stated that "*MAS does not currently regulate NFTs given the nature of their underlying assets*". Nevertheless, "*with regard to digital tokens such as NFTs, MAS takes a tech-neutral stance and 'looks through' to the underlying characteristics of the token to determine if it is to be regulated by MAS*".

For example, NFTs may be regulated by MAS if they have the characteristics of capital markets products under the Securities and Futures Act 2001 ("**SFA**").[13] Capital markets products include any securities, units in a collective investment scheme, derivatives contracts, spot foreign exchange contracts for the purposes of leveraged foreign exchange trading, and such other products as MAS may prescribe as capital markets products (Section 2(1) SFA).

To the extent that NFTs fall within the definition of DPTs in the PSA, they may also be regulated under the PSA. An NFT would be considered a DPT if it is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt (Section 2(1) PSA).

3.5 Are certain financial institutions or designated businesses required to maintain compliance programmes? What are the required elements of the programmes?

Yes. The requirements vary across industry sectors. Generally, FIs and Designated Businesses are required to maintain compliance programmes that reflect the nature and risk profiles of their business. Measures typically relate to CDD, reporting, recordkeeping, and internal policies, procedures and controls (see question 3.1 above). More details can be found below.

3.6 What are the requirements for recordkeeping or reporting large currency transactions? When must reports be filed and at what thresholds?

Requirements for recordkeeping vary across industry sectors.

FIs and other Designated Businesses must retain CDD information and other data, documents and information relating to a transaction for at least five years. FIs must also retain records of financial transactions for a minimum of five years (Section 43 CDSA).

PSM dealers must maintain records of cash transactions exceeding S$20,000, as well as customer information, for a period of five years (Section 67 CDSA and Section 18 Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 ("**PSPMA**")).[14]

PSPs must record adequate details of transactions that equal or exceed S$20,000 so that the transactions can be reconstructed (including the amount and type of currency involved) (Paragraph 16 of MAS Notice PSN01).

Reporting large currency transactions

A PSM dealer (or regulated dealer) must submit a CTR for cash transactions or designated transactions that exceed S$20,000 in a transaction (or in a day) (Section 17 PSPMA). For such transactions entered into before 10 April 2019, Section 68 of the CDSA applies (Section 40 PSPMA).

A pawnbroker must also submit a CTR with the STRO for the sale of any precious stone, precious metal or precious product to a customer for which cash (or a cash equivalent) exceeding S$20,000 is received as payment (Section 74A Pawnbrokers Act 2015).[15]

A casino operator is required to file a CTR with the STRO for cash transactions with a patron involving an aggregate amount of S$10,000 or more in a transaction (Regulation 3 Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009).[16]

3.7 Are there any requirements to report routinely transactions other than large cash transactions? If so, please describe the types of transactions, where reports should be filed and at what thresholds, and any exceptions.

Yes. STRs and CMRs are the other types of reports that may be filed with the STRO.

For when an STR must be filed, see question 3.11. For when a CMR must be filed, see question 3.8.

3.8 Are there cross-border transactions reporting requirements? Who is subject to the requirements and what must be reported under what circumstances?

Yes. A person who moves or attempts to move into or out of Singapore CBNIs exceeding S$20,000 (or the equivalent in foreign currency) must submit a CMR in respect of the movement.

A person who receives CBNIs from outside Singapore, for which the total value exceeds S$20,000 (or the equivalent in foreign currency), must submit a CMR in respect of the receipt within five business days (Sections 60 and 62 CDSA; Regulations 2A and 4A Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) Regulations 2007).[17]

3.9 Describe the customer identification and due diligence requirements for financial institutions and other businesses subject to the anti-money laundering requirements. Are there any special or enhanced due diligence requirements for certain types of customers?

CDD measures include:

(a) identifying and verifying the identity of the customer (or any beneficial owner in relation to the customer);
(b) understanding the purpose and intended nature of the business relationship with the customer; and
(c) ongoing monitoring of the business relationship with the customer.

A risk-based approach is commonly adopted. Enhanced CDD measures are required for politically exposed persons and their family members and close associates. Enhanced CDD measures are also required where the customer or beneficial owner is from or in a country that has been identified by the Financial Action Task Force ("**FATF**") as high risk, or which is known for having inadequate AML measures.

For such persons, enhanced CDD measures would be implemented, such as obtaining the approval of senior management before establishing or continuing business relations with the customer, taking reasonable measures to establish the customer's source of wealth and funds, and conducting enhanced ongoing monitoring of business relations with the customer.

Suspicious transaction reporting

Where any person knows or has reasonable grounds to suspect that any property is connected with drug dealing or criminal conduct, such knowledge or suspicion must be disclosed to the STRO as soon as reasonably practicable (see question 3.11).

There is no requirement to notify government authorities before reporting suspicious activity. The CDSA requires that STRs be made as soon as reasonably practicable after the information has come to the person's attention. However, FIs or Designated Businesses must also promptly extend a copy of the STR to MAS for their information (MAS Notices 626 Prevention of Money Laundering and Countering the Financing of Terrorism – Banks,[18] 824 Prevention of Money Laundering and Countering the Financing of Terrorism – Finance Companies,[19] 1014 Prevention of Money Laundering and Countering the Financing of Terrorism – Merchant Banks[20] and PSN01 Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services).[21]

Where any person (including an officer, employee or agent of that person) makes an STR disclosing their knowledge as soon as practicable after having that knowledge, they are deemed to not have been in possession of that information at any time (see Section 46 CDSA) for the purposes of determining liability for offences under CDSA Sections 50, 51, 53 and 54 (see question 1.2).

The information disclosed by an informer (defined as a person who makes an STR) as well as the identity of the informer are not to be disclosed in any civil or criminal proceedings, unless the court is of the view that the informer wilfully made a material statement that the informer knew or believed to be false or did not believe to be true, or that justice cannot be fully done between the parties to the proceedings without the disclosure of the name of the informer (Section 47 CDSA).

Section 45(7) of the CDSA further provides that good faith disclosure of information to the STRO is not a breach of any restriction upon disclosure, whether imposed by law, contract, or rules of professional conduct. The person shall not be liable for any loss arising out of the disclosure, or any act or omission in consequence of the disclosure.

3.10 Are financial institution accounts for foreign shell banks (banks with no physical presence in the countries where they are licensed and no effective supervision) prohibited? Which types of financial institutions are subject to the prohibition?

Yes, as below:

- Banks, finance companies and merchant banks are prohibited from entering into or continuing correspondent banking or other similar service relationships with foreign shell banks (MAS Notices 626 and 824).
- Capital markets intermediaries are prohibited from correspondent account service relationships with foreign shell banks (MAS Notice SFA04-N02 Capital Markets Intermediaries on Prevention of Money Laundering and Countering the Financing of Terrorism).[22]
- PSPs are prohibited from entering or continuing correspondent account services or other similar services relationship with shell FIs (MAS Notice PSN01).
- The CDP is prohibited from having correspondent account relations with foreign shell banks (MAS Notice SFA 03AA-N01 Depository on Prevention of Money Laundering and Countering the Financing of Terrorism).[23]
- Stored value facility holders are prohibited from having correspondent account service and other similar service relationships with foreign shell banks (MAS Notice PSOA-N02).

Each of the above FIs must also take appropriate measures when establishing the relevant relationship to satisfy itself that respondent FIs do not permit their accounts to be used by foreign shell banks.

3.11 What is the criteria for reporting suspicious activity?

If a person knows or has reasonable grounds to suspect that any property:

(a) in whole or in part, directly or indirectly, represents the proceeds of drug dealing/criminal conduct;

(b) was used in connection with drug dealing/criminal conduct; or

(c) is intended to be used in connection with any act that may constitute drug dealing/criminal conduct, and the information or matter on which the knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment,

then he must make an STR disclosing the knowledge or suspicion, or the information or other matter on which that knowledge or suspicion is based, as soon as is reasonably practicable after it comes to his attention (Section 45 CDSA).

3.12 What mechanisms exist or are under discussion to facilitate information sharing 1) between and among financial institutions and businesses subject to anti-money laundering controls, and/or 2) between government authorities and financial institutions and businesses subject to anti-money laundering controls (public-private information exchange) to assist with identifying and reporting suspicious activity?

(1) FIs in Singapore can share relevant information with branches and subsidiaries of the same financial group for risk management purposes, subject to appropriate safeguards. Such sharing may include information contained within an STR, the fact that an STR has been filed, and the STR itself.

On 1 April 2024, MAS launched COSMIC ("Collaborative Sharing of ML/FT Information & Cases"), a centralised digital platform to facilitate sharing of customer information among FIs to combat ML, FT and proliferation financing ("**PF**") globally. The legal basis and safeguards for such sharing are set out in the Financial Services and Markets (Amendment) Act 2023 and accompanying subsidiary legislation.[24] This will enable FIs to alert each other about potentially suspicious activity involving their customers and prevent persons from exploiting information gaps between FIs. FIs will also be able to review the risk information shared on the platform using data analytics.

Six major banks are participating in the ongoing initial phase, after which MAS intends to progressively extend the platform's coverage to more FIs.

(2) The Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership ("**ACIP**") was established in 2017 to bring together government authorities and FIs. ACIP comprises CAD, MAS, the Association of Banks Singapore and eight major banks. ACIP has published papers and held industry dialogues and workshops.

Following the recommendations of ACIP, CAD and MAS are taking steps to standardise data sets in STR and annual data collection, respectively, to allow for deeper analysis of data collected. They are also considering how standardised data sets and risk analytics can be shared with industry participants to help participants enhance their risk-based AML/CFT programmes.

In late 2019, ACIP held a workshop on the adoption of data analytics for enhancing AML/CFT effectiveness. Several ACIP member banks presented on how they had implemented data analytics to enhance their AML/CFT processes and key takeaways were drawn for the broader industry to benefit from.

3.13 Is adequate, current, and accurate information about the beneficial ownership and control of legal entities maintained and available to government authorities? Who is responsible for maintaining the information? Is the information available to assist financial institutions with their anti-money laundering customer due diligence responsibilities as well as to government authorities?

Recent efforts have been made to improve transparency on beneficial ownership and control.

Since 31 March 2017, most legal entities incorporated in Singapore have been required to maintain a private Register of Registrable Controllers ("**RORC**") at their registered office address, containing identification details of individuals and legal entities that have significant interest or significant control. For entities who are unable to identify such persons, they are required to identify individuals with executive control as their registrable controllers. Since 30 July 2020, most legal entities have also been required to lodge the information in their RORC with ACRA's Central Register of Controllers ("**ACRA's Central Register**"). If there are any changes to the information in the RORC, entities must first update their RORC before lodging the same information with ACRA's Central Register within two business days.

Since 5 December 2022, most legal entities have also been required to maintain a Register of Nominee Shareholders ("**RONS**") at their registered office address, which must contain particulars of the nominators of the company's nominee shareholders. If there are any changes to such information, legal entitles must also update the RONS accordingly within seven days of receiving notice.

The information in the RORC, RONS and ACRA's Central Register is only available to law enforcement agencies for the purpose of enforcing laws under their purview, such as the investigation of ML offences.

3.14 Is it a requirement that accurate information about originators and beneficiaries be included in payment orders for a funds transfer? Should such information also be included in payment instructions to other financial institutions? Describe any other payment transparency requirements for funds transfers, including any differences depending on role and domestic *versus* cross-border transactions.

Yes, the bank ordering the wire transfer must identify the wire transfer originator, verify that person's identity and record adequate details of the wire transfer. These requirements do not apply to a transfer and settlement between two FIs where both FIs are acting on their own behalf as the wire transfer originator and the wire transfer beneficiary (MAS Notices 626, 824, 1014 and PSN01).

Differences for domestic *versus* cross-border transactions

For cross-border wire transfers, the bank ordering the wire transfer must include in the payment instructions information such as the name and account number of both the wire transfer originator and wire transfer beneficiary, as well as the wire transfer originator's residential address, or registered or business address, unique identification number or the date and place of birth, incorporation or registration of the wire transfer originator if the amount to be transferred exceeds S$1,500 (MAS Notices 626, 824 and 1014).

For domestic wire transfers, the bank ordering the wire transfer must include in the payment instructions information such as the name and account number of the wire transfer originator and the wire transfer originator's residential address, or registered or business address, unique identification number or the date and place of birth, incorporation or registration of the wire transfer originator (MAS Notices 626, 824 and 1014).

Nevertheless, the bank may include only the wire transfer originator's account number provided that it will permit the transaction to be traced back to the wire transfer originator and wire transfer beneficiary, and the bank is able to provide the wire transfer originator information set out in the preceding paragraph upon request by the beneficiary institution, MAS, law enforcement authorities or other relevant authorities in Singapore (MAS Notices 626, 824 and 1014).

3.15 Is ownership of legal entities in the form of bearer shares permitted?

No, it is not permitted (see Sections 66 and 364 Companies Act 1967).[25]

3.16 Are there specific anti-money laundering requirements applied to non-financial institution businesses, e.g., currency reporting?

Yes, such requirements are applied (see question 3.1).

3.17 Are there anti-money laundering requirements applicable to certain business sectors, such as persons engaged in international trade or persons in certain geographic areas such as free trade zones?

The regulatory requirements are targeted at specific industries (see questions 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.9, 3.10 and 3.14).

3.18 Are there government initiatives or discussions underway regarding how to modernise the current anti-money laundering regime in the interest of making it more risk-based and effective, including by taking advantage of new technology, and lessening the compliance burden on financial institutions and other businesses subject to anti-money laundering controls?

Yes. The Government Technology Agency of Singapore has developed MyInfo, a digital platform containing personal data verified by the government. As of mid-2021, close to 700 digital services offered by government agencies and businesses, including FIs and Designated Businesses, had implemented MyInfo. MyInfo removes the need for customers to submit physical identification documents to FIs and Designated Businesses for verification purposes, as the information in MyInfo can be used and relied upon instead. FIs and Designated Businesses that use MyInfo when onboarding customers enjoy a reduced compliance burden as a result.

The government has also actively encouraged the private sector to use and develop new technology to combat ML. In August 2020, MAS committed S$250 million over the following three years under the enhanced Financial Sector Technology and Innovation Scheme to accelerate technology and innovation-driven growth in the financial sector, which includes the use of technology to combat ML. On 1 April 2024, MAS also launched COSMIC, a digital information-sharing platform for FIs.

4 General

4.1 If not outlined above, what additional anti-money laundering measures are proposed or under consideration?

In July 2021, MAS issued a consultation paper to obtain feedback on a proposed new AML/CFT Notice for FIs dealing in PSM and updates to existing AML/CFT Notices to enhance the mitigation of ML risks in the sector. In March 2022, MAS published the results of the consultation, stating that respondents were generally supportive of MAS's proposals, which have since been adopted. This includes a new Notice for FIs dealing in PSM, as well as amendments to align existing AML/CFT requirements for digital token services provided by various FIs (including banks, merchant banks, finance companies and credit card or charge card licensees) with that for DPT service providers, and enhanced CDD measures to assess whether a customer may be a shell company that presents higher ML risks.

4.2 Are there any significant ways in which the anti-money laundering regime of your country fails to meet the recommendations of the Financial Action Task Force ("FATF")? What are the impediments to compliance?

No. In the FATF's last Mutual Evaluation Report relating to the implementation of AML/CFT standards in Singapore, published in 2019, Singapore was compliant or largely compliant with 37 of the FATF's 40 Recommendations.

4.3 Has your country's anti-money laundering regime been subject to evaluation by an outside organisation, such as the FATF, regional FATFs, Council of Europe (Moneyval) or IMF? If so, when was the last review?

Yes. The last review was in 2019 (see question 4.2). The relevant report can be obtained here: https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-singapore-2019.html.

4.4 Please provide information on how to obtain relevant anti-money laundering laws, regulations, administrative decrees and guidance from the Internet. Are the materials publicly available in English?

The relevant AML laws, regulations, administrative decisions, and guidance can be obtained from various official websites. These include Singapore Statutes Online,[26] the STRO's website[27] and MAS's website.[28]

Endnotes

1. https://sso.agc.gov.sg/Act/CDTOSCCBA1992
2. https://sso.agc.gov.sg/Act/OCA2015
3. https://sso.agc.gov.sg/Act-Rev/BA1970/Published/20211231?DocDate=20080331&WholeDoc=1
4. https://sso.agc.gov.sg/Act/MASA1970
5. https://sso.agc.gov.sg/Act/CPC2010?ProvIds=P17A-#pr149D-
6. https://acd.mlaw.gov.sg/guidelines
7. https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Enforcement-Monograph-Sep-2018-v2.pdf?la=en&hash=7E3D30EE8EBF024C287E6CAEB7D5F8BA78251091
8. https://sso.agc.gov.sg/Acts-Supp/18-2022/Published/20220511?DocDate=20220511&WholeDoc=1#pr8-
9. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-fit-and-proper-criteria
10. https://sso.agc.gov.sg/Act/PSA2019
11. https://www.mas.gov.sg/regulation/notices/psn01-aml-cft-notice---specified-payment-services?scid=s7_6AqR0Mk&id=M9Pm7cMxbA
12. https://www.mas.gov.sg/regulation/notices/psn02-aml-cft-notice---digital-payment-token-service
13. https://sso.agc.gov.sg/Act/SFA2001?ProvIds=P11-#pr2-
14. https://sso.agc.gov.sg/Act/PSPMPMLTFA2019
15. https://sso.agc.gov.sg/Act/PA2015?WholeDoc=1
16. https://sso.agc.gov.sg/SL/CCA2006-S507-2009?DocDate=20190603&ProvIds=pr3-#pr3-
17. https://sso.agc.gov.sg/SL/CDTOSCCBA1992-S595-2007?DocDate=20160629#pr2A-
18. https://www.mas.gov.sg/regulation/notices/notice-626
19. https://www.mas.gov.sg/regulation/notices/notice-824
20. https://www.mas.gov.sg/regulation/notices/notice-1014
21. https://www.mas.gov.sg/regulation/notices/psn01-aml-cft-notice---specified-payment-services
22. https://www.mas.gov.sg/regulation/notices/notice-sfa-04-n02
23. https://www.mas.gov.sg/regulation/notices/notice-sfa-03aa-n01
24. https://sso.agc.gov.sg/Acts-Supp/19-2023/Published/20230628?DocDate=20230628
25. https://sso.agc.gov.sg/Act/CoA1967
26. https://sso.agc.gov.sg
27. https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office
28. https://www.mas.gov.sg

Gary Low is the Co-Head of the Firm's Criminal Law Practice. He practises both civil and criminal litigation. He has an active civil/commercial practice and has acted in a wide variety of matters, including disputes in banking and finance, commercial disputes, arbitrations, directors'/shareholders' disputes, minority oppression, tortious liability, property and contractual disputes.
Gary has also represented clients for commercial crimes, corruption and securities offences such as insider trading and market manipulation. He has also advised on AML practices and been involved in investigations by various corporations into alleged wrongdoings of employees in relation to fraud, criminal breach of trust, cheating, breach of fiduciary duties and other misconduct. Gary is a recommended lawyer in multiple publications such as *The Legal 500 Asia Pacific* (Dispute Resolution), *Who's Who Legal* (Business Crime Defence – Corporates), *Global Investigations Review 100* and *Benchmark Litigation Asia Pacific* (Commercial and Transactions, White Collar Crime).

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 2497
Email: gary.low@drewnapier.com
LinkedIn: www.linkedin.com/in/gary-low-58b6a11

Terence Tan has experience handling a wide range of corporate, commercial and other complex disputes in litigation and arbitration. His practice focuses on disputes involving company directors and/or shareholders, minority oppression, breaches of fiduciary or directors' duties, civil fraud and conspiracy, banking and finance, and technology.
Terence also has an active criminal law practice involving a diverse array of commercial and non-commercial criminal offences and has assisted clients with investigations to identify wrongdoing by employees. Terence is a recommended lawyer in publications including *The Legal 500 Asia Pacific* and *asialaw Leading Lawyers*.

Drew & Napier LLC
10 Collyer Quay
10th Floor Ocean Financial Centre
Singapore 049315

Tel: +65 6531 2378
Email: terence.tan@drewnapier.com
LinkedIn: www.linkedin.com/in/terence-tan-3073a072

Drew & Napier's Criminal Practice comprises an exceptional team of specialists from across the firm's practice groups, including Banking & Corporate, Tax, Intellectual Property and Dispute Resolution. We provide our clients with a single access point for representation on commercial, securities, and non-commercial crimes. Our lawyers have dealt with an extensive range of criminal matters and have experience in regulatory, trial and appeal processes. We are committed to providing support for our clients at every stage of the criminal justice process, from investigations to prosecutions in court. Our clients include major corporations, listed companies and individuals.
In 2020, Drew & Napier united with some of the most influential leading law firms in Southeast Asia to form a network of blue-chip law firms – Drew Network Asia (DNA). Comprising legal powerhouses Shearn Delamore & Co. from Malaysia, Makarim & Taira S. from Indonesia, Martinez Vergara & Gonzalez Sociedad (MVGS) from the Philippines, Tilleke & Gibbins, established in Cambodia, Laos, Myanmar, Thailand and Vietnam, alongside Drew & Napier, DNA is a cohesive and integrated team operating as "a firm of firms" with international perspective and strong local expertise. Learn more about DNA at www.drewnetworkasia.com.

www.drewnapier.com

DREW & NAPIER

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Anti-Money Laundering 2024 features five expert analysis chapters and 19 Q&A jurisdiction chapters covering key issues, including:

- The Crime of Money Laundering and Criminal Enforcement
- Anti-Money Laundering Regulatory/Administrative Requirements and Enforcement
- Anti-Money Laundering Requirements for Financial Institutions and Other Designated Businesses

The International Comparative Legal Guides are published by: glg Global Legal Group