International
Comparative
Legal Guides

Anti-Money Laundering 2021

A practical cross-border insight into anti-money laundering law

Fourth Edition

Featuring contributions from:

Anagnostopoulos
Bae, Kim & Lee LLC
Bonifassi Avocats
BSA Ahmad Bin Hezeem & Associates LLP
Cadwalader, Wickersham & Taft LLP
City Legal
DQ Advocates Limited
Drew & Napier LLC
Enache Pirtea & Associates
Fabio Humar Abogados
Galicia Abogados, S.C.
Geijo & Associates
Gibson, Dunn & Crutcher LLP
Herbert Smith Freehills LLP
JahaeRaymakers
Joyce Roysen Advogados
Kellerhals Carrard Zürich KlG
King & Wood Mallesons
Kobre & Kim LLP
Linklaters LLP
Marxer & Partner Attorneys at Law
Matheson
Morais Leitão, Galvão Teles, Soares da Silva & Associados
Nakasaki & Sato Law Firm
Nyman Gibson Miralis
Portolano Cavallo
S. U. Khan Associates Corporate & Legal Consultants
Threshing Fields Law
White & Case LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Singapore


Gary Low


Victor David Lau

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 (Cap. 65A) ("**CDSA**").

The relevant ML offences are found in Sections 43, 44, 46, 47 and 47AA of the CDSA. Although these provisions do not use the term "money laundering" *per se*, they criminalise the dealing in property which represents, in whole or in part, directly or indirectly, the benefits of drug dealing and criminal conduct ("**ML Proceeds**").

Sections 46(1) and 47(1) of the CDSA impose strict liability on acquiring, possessing, using, concealing or transferring of the accused's own ML Proceeds. The PP would need to prove that the accused had:

(a) concealed or disguised his ML Proceeds;
(b) converted or transferred his ML Proceeds or removed them from the jurisdiction; or
(c) acquired, possessed, or used his ML Proceeds.

Sections 46(2) and 47(2) of the CDSA provide for the offences of concealing, disguising, converting, transferring, or removing from the jurisdiction another person's ML Proceeds. The PP would need to prove that the accused had carried out such acts, and that the accused did so knowing or having reasonable grounds to believe that the property was another person's ML Proceeds.

Sections 46(3) and 47(3) of the CDSA provide for the offences of acquiring, possessing, or using another person's ML proceeds. The PP must prove that the accused had carried out such acts, and that the accused did so knowing or having reasonable grounds to believe that the property was another person's ML Proceeds.

Section 47AA of the CDSA provides for the offence of possessing or using any property which may reasonably be suspected to be ML Proceeds. The PP would only need to prove that the accused had carried out such acts, and that the property would be suspected by a reasonable person to be ML Proceeds. The accused has to account satisfactorily for how he came to possess/use the property, or otherwise be guilty of the offence.

Sections 43 and 44 of the CDSA provide for the offences of assisting another person to retain their ML Proceeds. 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 knowing or having reasonable grounds to believe that:

(a) the arrangement would:
  (i) facilitate in the retention or control of the other person's ML Proceeds by or on behalf of the other person, whether by concealment, removal from jurisdiction, transfer to nominees, or otherwise;
  (ii) use the other person's ML Proceeds to secure funds that are placed at that other person's disposal, directly or indirectly; or
(b) use the other person's ML Proceeds for the other person's benefit to acquire property by way of investment or otherwise; or 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

There are numerous predicate offences for ML.

The first category of predicate offences is "drug dealing offences", which are listed in the First Schedule of the CDSA. The second category of predicate offences is "serious offences", which are listed in the Second Schedule of the CDSA.

Predicate offences also include foreign drug dealing or foreign serious offences, i.e. an offence against the law of a foreign country, which would also constitute an offence listed in the First or Second Schedules of the CDSA if the conduct occurred in Singapore (Section 2(1) CDSA).

Whether tax evasion is a predicate offence for money laundering

Yes. Tax evasion under Singapore law and the national law of a foreign country in certain specified forms are predicate offences for ML (Section 2(1) and Second Schedule 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 can apply regardless of whether the predicate offences take place in Singapore or elsewhere (see question 1.2 above on foreign drug dealing and foreign serious offences).

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**"), which sits within 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.

The PP and the officers of the Attorney-General's Chambers acting under the authority of the PP prosecute ML offences in consultation with the aforementioned investigative agencies.

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 43, 44, 46 and 47 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 drug dealing/criminal conduct in respect of which the offence was committed, whichever is higher.

The maximum penalty under Section 47AA 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 that the court considers 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?

There is no separate forfeiture/confiscation authority.

When a defendant is convicted of one or more predicate offences in the CDSA, the PP may apply to the court for a confiscation order. Benefits derived from the defendant from his or her drug dealing/criminal conduct will be subject to a confiscation order if the court is satisfied that such benefits have been so derived (Sections 4 and 5 CDSA).

Where there has been no criminal conviction, material/financial gains from organised crime activity can still be confiscated under the Organised Crime Act 2015 (No. 26 of 2015) ("**OCA**"). The confiscation order under the OCA does not require that the organised crime activity be the subject of any criminal proceedings (Section 51 OCA). In fact, 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.

"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 43, 44, 46 and 47 of the CDSA) and is carried out at the direction of/in furtherance of the illegal purpose of a group which the person knows or has reasonable grounds to believe is an (locally linked) organised criminal group (Section 48(1)(a)–(b) OCA). It 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 of the OCA).

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

While it is uncommon for banks and other regulated financial institutions ("**FIs**") to be formally charged and convicted in court for ML offences, officers and employees of FIs have previously been convicted in court for such 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**"). 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 1MDB case.

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?

Certain specified criminal actions against a company, partnership or unincorporated association, including those in respect of offences under Sections 43, 44, 46, and 47 of the CDSA, may be resolved through Deferred Prosecution Arrangements ("**DPAs**") (Part VIIA of the Criminal Procedure Code (Cap. 65A)).

A DPA comes into force only when the High Court approves it by making a declaration that the DPA is in the interests of justice, and that its terms are fair, reasonable, and proportionate. After such approval, the DPA is published.

DPAs are not available to individuals.

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.

The Monetary Authority of Singapore ("**MAS**") imposes anti-money laundering ("**AML**") requirements on FIs in Singapore.

Other authorities impose AML requirements on non-financial businesses and professions, such as:

- the Casino Regulatory Authority of Singapore (for casinos);
- the Accounting and Corporate Regulatory Authority ("**ACRA**") (for corporate service providers, public accountants and accounting entities); and
- the Council for Estate Agents (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 (Cap. 161) (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? If so, are the criteria for examination publicly available?

MAS enforces AML requirements under MAS-administered laws and regulations. Reference can be made to the MAS Enforcement Monograph which outlines MAS's approach to enforcement, and the various MAS guidelines on AML.

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, analyses and disseminates suspicious transaction reports ("**STRs**"), cash transaction reports ("**CTRs**") and physical currency and bearer negotiable instruments ("**CBNIs**") reports ("**CBNIRs**").

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

There is no limitation period for enforcement actions.

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.

An FI that fails to comply with any AML direction issued or regulation made by MAS is liable to a fine not exceeding S$1,000,000, 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 (Section 27B(2) of the Monetary Authority of Singapore Act (Cap. 186)).

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 can impose sanctions such as:

- revocation or suspension of licences;
- removals of directors and officers;
- prohibition orders ("**POs**") barring persons from conducting regulated activities or from taking part in management of the 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 FIs, failing to comply with their AML obligations is an offence (see question 2.8).

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, but rarely pursued in practice. Typically, most resolutions of penalty actions are published by the relevant regulatory authority. As penalty assessments are usually composition fines, FIs cannot, by the nature of the composition of offences, challenge them.

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

3.1 What financial institutions and other businesses are subject to anti-money laundering requirements? Describe which professional activities are subject to such requirements and the obligations of the financial institutions and other businesses.

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 businesses subject to AML requirements ("**Designated Businesses**") include:

- casino operators;
- corporate service providers;
- dealers in precious stones and/or precious metals ("**PSMDs**");
- estate agents and salespersons;
- legal practitioners and law practices;
- moneylenders;
- payment service providers ("**PSPs**");
- pawnbrokers; and
- professional accountants and professional accounting firms (including public accountants and accounting entities).

The applicable AML obligations are set out in specific statutes, subsidiary legislation, directions, guidelines, codes, and practice notes/circulars. They generally require FIs or Designated Businesses 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.

3.2 To what extent have anti-money laundering requirements been applied to the cryptocurrency industry?

Under the Payment Services Act (No. 2 of 2019), cryptocurrency companies (also known as Digital Payment Token ("**DPT**") service providers), including exchanges, are obliged to register and apply for a PSP licence. They must also meet the AML/countering the financing of terrorism ("**CFT**") requirements under MAS Notice PSN02. On 4 January 2021, the Payment Services (Amendment) Bill was passed to expand the licensing regime to service providers of DPTs that may not themselves possess DPTs (also known as Virtual Assets Service Providers ("**VASPs**")).

3.3 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.

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

Recordkeeping

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 37 CDSA).

PSMDs must maintain records of cash transactions exceeding S$20,000, as well as customer information, for a period of five years (Section 48I CDSA; Section 18 Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 ("**PSPMA**")).

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 PSMD (or regulated dealer) must submit a CTR for cash transactions or designated transactions which exceed S$20,000 in a transaction (or in a day) (Section 17 PSPMA).

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 of the Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009).

3.5 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 CBNIRs are the other types of reports that may be filed with the STRO.

For when a STR must be filed, see question 3.9. For when a CBNI Report must be filed, see question 3.6.

3.6 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 CBNI exceeding S$20,000 (or its equivalent in a foreign currency) must make a CBNIR in respect of the movement. A person who receives CBNI from outside Singapore the total value of which exceeds S$20,000 (or its equivalent in a foreign currency) must make a CBNI Report in respect of the

receipt within five business days (Sections 48C and 48E CDSA, and regulations 2A and 4A, Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) Regulations 2007).

Limited exemptions to the above reporting requirements are set out in Sections 48C(7) and 48C(8) of the CDSA and the Corruption, Drug Trafficking and Other Serious Crimes (Cross Border Movements of Physical Currency and Bearer Negotiable Instruments) (Exemption) Orders 2007 and 2010.

3.7 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 individuals, 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.

3.8 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. 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 Notice 626). Capital markets intermediaries are prohibited from correspondent account service relationships with foreign shell banks (MAS Notice SFA04-N02). Money-changing and remittance business licensees are prohibited from providing remittance services to foreign shell banks (MAS Notice 3001). The CDP is prohibited from having correspondent account relations with foreign shell banks (MAS Notice SFA03AA-N01). Stored value facility holders are prohibited from 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.

3.9 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; (b) was used in connection with; or (c) is intended to be used in connection with, any act which 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 a 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 39 CDSA).

3.10 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?

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 a STR, the fact that an STR has been filed, and the STR itself.

To facilitate public-private information exchange, the Anti-Money Laundering and Countering the Financing of Terrorism Industry Partnership ("**ACIP**") was established in 2017, comprising the Association of Banks Singapore, eight major banks, CAD, and MAS.

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 end-2018, ACIP's Data Analytics Working Group launched a paper to share the experiences of ACIP member banks in using data analytics techniques to combat financial crime. Successful and less successful pilots by member banks were discussed and lessons were drawn for the broader industry to benefit from.

3.11 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 are 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. By 30 June 2021, most legal entities will also have to lodge the information in their RORC with the ACRA's Central Register of Controllers ("**ACRA's Central Register**").

Entities have an obligation to ensure that the information in its RORC and the ACRA's Central Register are up to date. On an annual basis, entities are required to send notices to all

controllers to verify whether there are any relevant changes to the particulars of the controllers. Non-compliance is a criminal offence for the entity as well as the controller.

The information in the RORC and the ACRA's Central Register are only available to law enforcement agencies.

3.12 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?

Yes, the bank ordering the wire transfer must identify the wire transfer originator, verify his 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 3001).

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

No (see Sections 66 and 364 of the Companies Act (Cap. 50)).

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

Yes (see question 3.1).

3.15 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, 3.7, 3.8, and 3.12).

3.16 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, which is a digital platform containing personal data verified by the government. MyInfo potentially 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 would enjoy a reduced compliance burden as a result. The platform is progressively being made available to a wider range of business transactions after a successful pilot with several banks, where the use of MyInfo shortened the time taken to open a bank account by as much as 80%.

The government has also actively encouraged the private sector to use and develop new technology to combat ML. ACIP has published a paper studying the use of data analytics for AML/CFT measures (see question 3.10). On 13 August 2020, the MAS committed S$250 million over the next three years under the enhanced Financial Sector Technology and Innovation Scheme ("**FSTI 2.0**") to accelerate technology and innovation-driven growth in the financial sector, which includes the use of technology to combat ML.

4 General

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

In July 2020, the MAS published a consultation paper to obtain feedback on a proposed new Omnibus Act which would enhance and consolidate MAS's regulatory powers in relation to FIs and digital services. The proposed Omnibus Act also contains a harmonised and expanded power to issue POs, a new part on the regulation of VASPs created in Singapore for AML/CFT purposes, and a harmonised power to impose requirements on technology risk management. As of the time of writing, the results of the consultation have not yet been published.

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 and CFT standards in Singapore, published in 2019, Singapore was compliant or largely compliant for 37 of the FATF 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 (see question 4.2 above).

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 (http://sso.agc.gov.sg/) and MAS's website (http://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
URL: www.drewnapier.com

Victor David Lau practises both civil and criminal litigation. He has acted and assisted in a broad range of matters, including commercial disputes, arbitrations, directors'/shareholders' disputes, criminal/corruption trials, defamation and property disputes.
Prior to joining legal practice, Victor was a regulatory and enforcement officer at Enterprise Singapore and the Competition & Consumer Commission of Singapore.

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

Tel: +65 6531 2491
Email: victordavid.lau@drewnapier.com
URL: www.drewnapier.com

ICLG.com

Other titles in the ICLG series

Alternative Investment Funds
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group