Expert Analysis: Singapore's Regime on Anti-Money Laundering and Countering the Financing of Terrorism

This report was originally published on
Thomson Reuters Regulatory Intelligence.

THOMSON REUTERS®

Singapore's openness as an international transport hub and financial centre presents inherent risk exposure to cross-border money-laundering and terrorism financing opportunities. While a strict legislative framework is in place to deal with such risks, businesses which are internationally-oriented and cash-intensive nonetheless remain vulnerable, and include retail and private banks, remittance agents, money-changers, internet-based stored value facility holders, corporate service providers, casinos and pawn brokers.

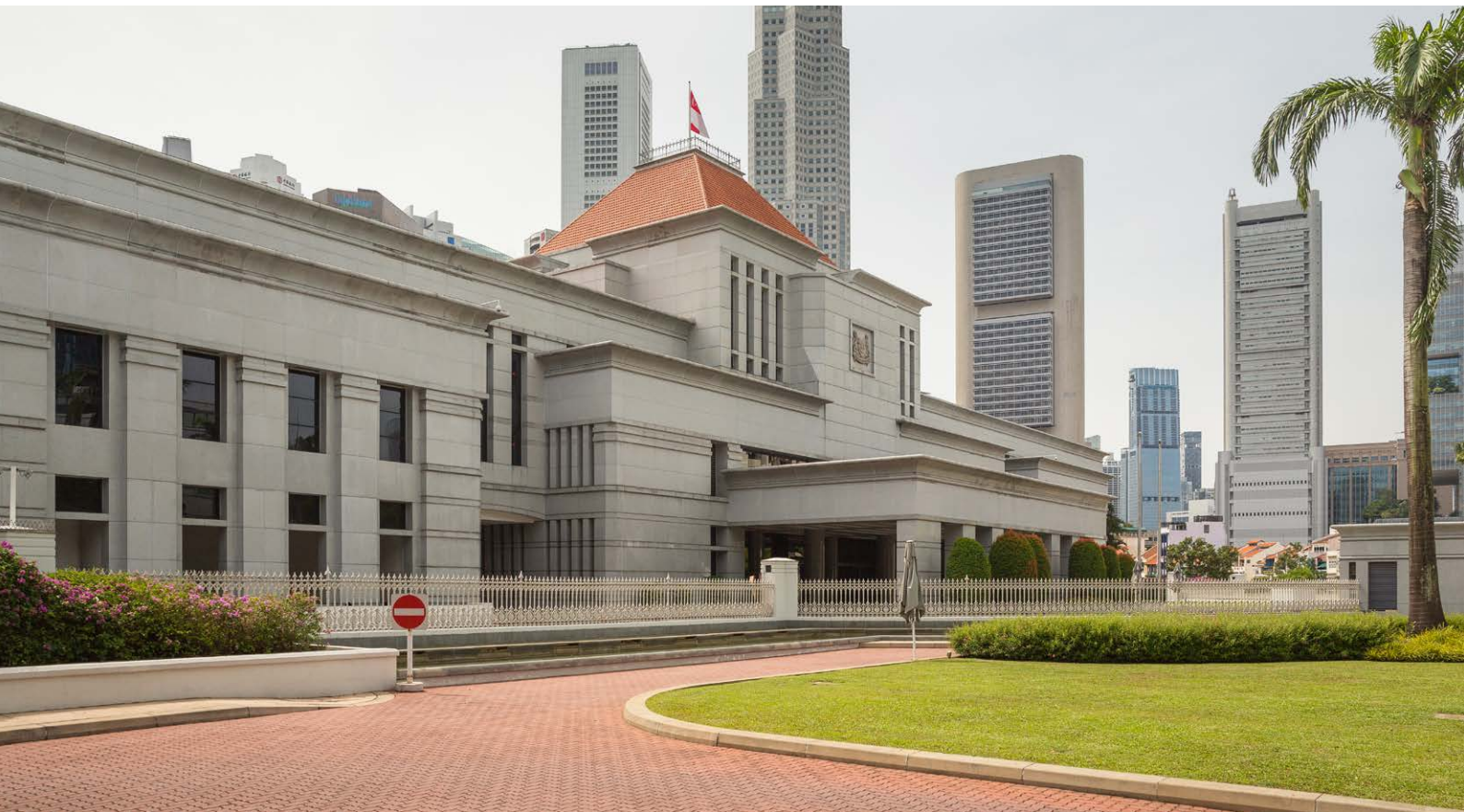
Legislative framework

Singapore's anti-money laundering and countering the financing of terrorism regime consists of various pieces of legislation, providing for a broad range of serious offences for which a money laundering charge can apply. Soft laws, such as notices and guidance papers issued by the Monetary Authority of Singapore setting out practices which financial institutions must abide by also contribute to Singapore's robust regime.

The two key pieces of legislation dealing with anti-money laundering (AML) and countering the financing of terrorism (CFT) activities are the (1) Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap 65A) (CDSA); and (2) Terrorism (Suppression of Financing) Act (Cap 325) (TSFA).

Other pieces of legislation have also been enacted which contribute to the overall legislative framework – for example, under the Moneylenders Act (Cap 188), the act of receiving, possessing, concealing or disposing of any funds or other property, or engaging in a banking transaction relating to any funds, on behalf of another person known or reasonably believed to be carrying on an unlicensed money lending business attracts a fine of between S$30,000 and S$300,000 and imprisonment of up to seven years for repeat offenders. This indirectly targets money-laundering operations by crippling activities commonly employed in such operations.

This report will examine the offences under the CDSA and TSFA, and the risk based approach for the performance of client due diligence or know your client checks by financial institutions.



Offences

The CDSA

The offences under the CDSA can be divided into primary and secondary offences. Primary offences are those which involve the actual act of money laundering. Secondary offences are those which do not involve acts of money laundering per se; instead, the offences cover acts or omissions which encourage money laundering. There are two primary offences under the CDSA, and it is an offence for a person to:

- enter into an arrangement that allows or facilitates another person to retain, control or invest the benefits of drug trafficking or criminal conduct where the person knows or has reasonable grounds to believe that the other person may be a drug trafficker or involved in criminal conduct or has benefited from such activities (for example, entering into an arrangement with a criminal to assist with the laundering of benefits from drug dealing or from criminal conduct); and
- acquire, possess, use, conceal, disguise, transfer or remove from Singapore any property that represents, or if there is knowledge or reasonable grounds to believe that the property represents the proceeds of drug trafficking or criminal conduct.

The CDSA was amended in 2012 to remove the requirement that the acquisition of proceeds of drug trafficking and criminal conduct should be for no or inadequate consideration. This is to avoid informed criminals from intentionally acquiring proceeds of drug trafficking or criminal conduct at fair value to escape prosecution. The CDSA was further amended in 2014 to make such that it is not necessary for all the particulars of any offence to be proven in order to prove an offence under the CDSA. What this means is that if a case contains enough (but not all) particulars, an offence under the CDSA can be made out.

A further amendment of the CDSA in 2019 had similar effect. If the act constituting a drug dealing or criminal conduct offence occurred in a foreign country, it will be presumed to constitute such an offence if the prosecution adduces satisfactory evidence that the act fulfils all elements of a foreign drug dealing offence or foreign serious offence. The presumption remains until the contrary is proved.

In addition, a new offence criminalises possession of property if the property is reasonably suspected of representing benefits from money laundering, and the person fails to account satisfactorily how he came by the property.

Secondary offences include:

- the failure to report information (in the form of a suspicious transaction report obtained during the course of an individual's trade, profession, business or employment, which relates to property, in whole or in part or, directly or indirectly which the individual knows or has reasonable grounds to believe was used in connection with or is intended to be used in connection with an act that may constitute drug trafficking or criminal conduct; and
- "tipping off".

The CDSA was also amended in 2012 to the effect that where the suspected property is the subject of a transaction, the obligation to report arises regardless of whether the transaction involving the said property was completed.

The offence of "tipping off" under the CDSA

Under the CDSA, a person will be guilty of the "tipping off" offence if the person knows or has reasonable grounds to suspect that:

- that an authorised officer under the CDSA is acting (or is proposing to act) in an investigation for the purposes of the CDSA; or
- a disclosure has been made to an authorised officer under the CDSA (usually the suspicious transactions reporting officer (STRO)),
- discloses to any other person information which is likely to prejudice any investigation or proposed investigation.

The CDSA was amended in 2014 to extend legal professional privilege to legal counsels. Certain communications and documents prepared in connection with a legal counsel providing advice to his employer or relating to any legal proceedings in which the employer is or may be a party will be subject to legal professional privilege.

Tipping off and suspicious transactions reporting

The CDSA was amended in 2014 that obliges the government to formally establish a Suspicious Transaction Reporting Office (STRO).

The United Kingdom's AML regime provides that the STRO equivalent in UK should give or refuse consent to the disclosing party to continue with the suspected transaction within seven clear working days from the date the suspicious transaction report (STR) is lodged.

If there is no response after seven days, there will be deemed consent for the disclosing party to act. If consent is withheld, the disclosing party must not continue with the transaction for a further period of 31 calendar days from the date of the refusal.

Singapore's AML regime does not have this mechanism, and this may expose the disclosing party to potential criminal prosecution by the relevant authorities. For example, a banker (the "informer") discovers or has reasonable grounds to believe that Mr X is involved in money laundering, and has deposited suspected criminal proceeds with his bank. A STR has been lodged immediately by the Informer and Mr X comes the next day to instruct the Informer to wire transfer the monies to one Mr Y.

If he complies with Mr X's instruction, he may be at risk of committing the primary offences under the CDSA. If he refuses to comply, he could face prosecution for the "tipping off" offence because his refusal may alert Mr X to the possibility of a STR being lodged against him, or there are investigations or pending investigations against the proceeds.

A further difficult situation might arise if Mr X enquires about the reason behind the informer's or the bank's refusal or delay in carrying out his instructions, which will place them in an unenviable position of having to provide a "truthful" account to Mr X without tipping him off.

Prior to amendments in the CDSA in 2014, the bank may also be exposed to civil claims for failing to carry out Mr X's instructions. However, this risk of civil claims against the bank is someone mitigated with the 2014 amendments to the CDSA which provide that the bank will not be liable for any loss arising out of the disclosure or any act or omission in consequence of the any disclosure which the STRO might require the bank to make.

Penalties under the CDSA

Penalties for offences contained in the CDSA were increased in 2019. It should be noted that penalties for legal persons have particularly increased to reflect their greater level of culpability. For primary money laundering offences, the penalty for individuals is a fine of up to S$500,000 or 10 years' imprisonment, or both. For legal persons, it is a fine of up to the higher of S$1,000,000 or twice the value of the benefits of the drug dealing or criminal conduct involved. For the possession or usage of property representing any benefits of money laundering without satisfactory explanation, the penalty for individuals is a fine of up to S$150,000 or three years' imprisonment, or both.

For legal persons, it is a fine of up to S$300,000. For secondary offences, the failure to report knowledge or suspicion of money laundering will attract a fine of up to S$250,000 or three years' imprisonment, or both, if the person is an individual. For legal persons, it is a fine of up to S$500,000. Last, the offence of "tipping off" entails a fine of up to S$250,000 or three years' imprisonment, or both upon conviction.

The TSFA

There are six primary offences under the TSFA, and it is an offence for a person to:

- provide or collect property that will be used to commit any terrorist act, knowing or having reasonable grounds to believe that the property, in whole or in part, will be used for that purpose;
- collect property, provide or invite a person to provide, or make available property or financial or other related services, intending that they will be used for a terrorist act, or knowing or having reasonable grounds to believe that they will be used for a terrorist act, or for the benefit of the person carrying out a terrorist act, or to benefit any terrorist or terrorist entity;
- use or possess any property which in whole or in part will be used for terrorist purposes;
- deal directly or indirectly in any terrorist-owned property;
- enter into or facilitate directly or indirectly any financial transaction that relates to any terrorist property; and
- provide any financial or other related services in respect of any property belonging to a terrorist, or for the benefit of or on the direction of any terrorist or terrorist entity.

Acting reasonably in taking, or omitting to take, measures to avoid committing such offences is a defence in any civil proceedings arising from taking or omitting to take those measures.

In 2013, the TSFA was amended to include the following new provisions which:

- makes it an offence to disclose, by one person to another, information which is likely to prejudice the investigation of a terrorism financing offence (similar to the offence of tipping off under the CDSA);
- protects the identity of informers against disclosure and discovery during legal proceedings.

The TSFA was amended in 2019 to clarify that 'carrying out' a terrorist act includes references to financing the travel of an individual to any place (besides his place of citizenship or residence), in order for the individual to provide or receive any training in facilitating or carrying out any terrorist act. Also, the

2019 amendment made it an offence to abet, conspire, or attempt to commit the above six primary offences—whether via committing an act or omission.

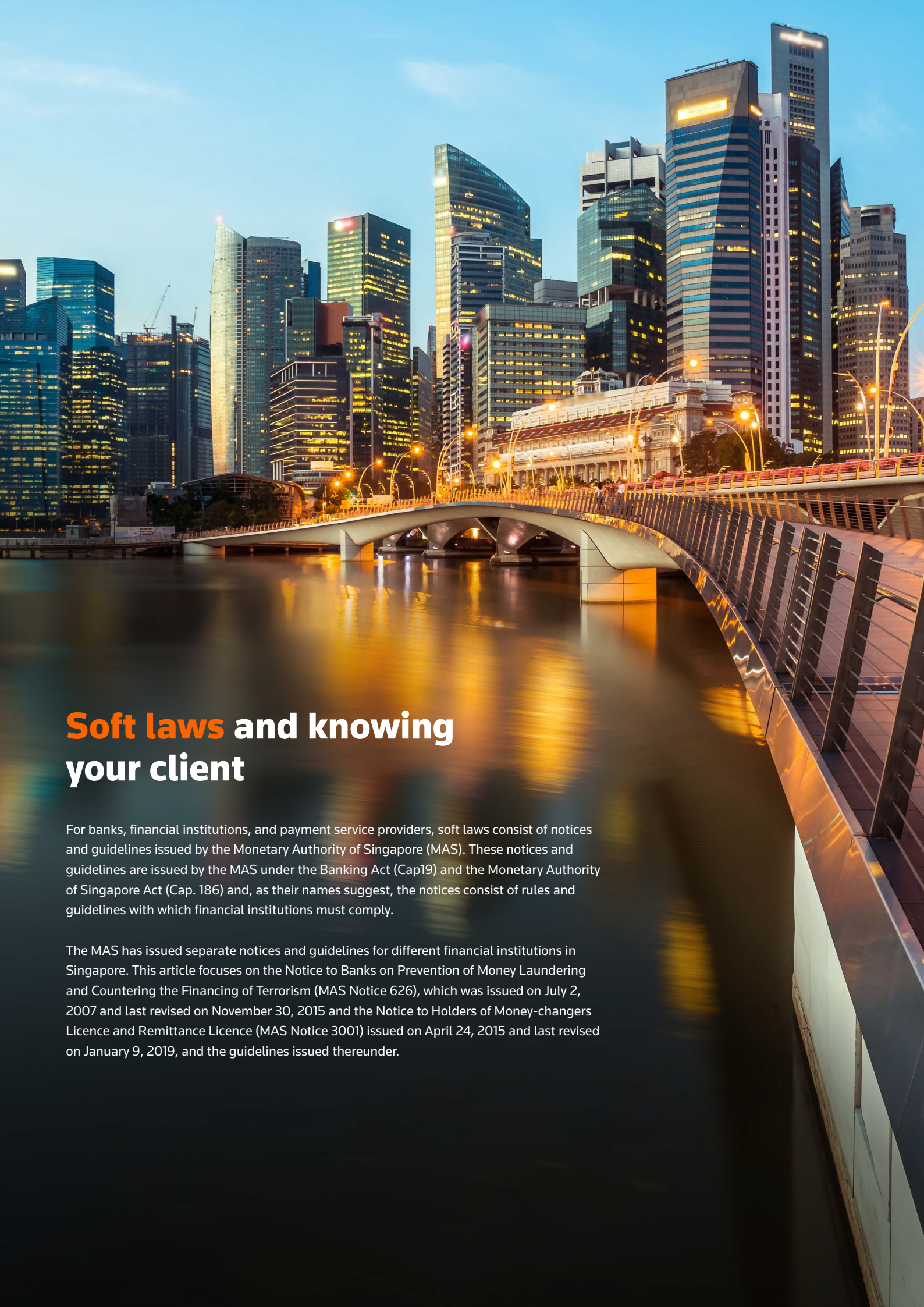
Similar to the CDSA, the TSFA also imposes reporting obligations which require any person who has in their possession, custody or control any property which belongs to any terrorist or terrorist entity, or any information about any transaction or proposed transaction relating to terrorist property, to inform the Commissioner of Police of such information.

Penalties under the TSFA

Penalties for offences contained in the TSFA were increased in 2019. For individuals, the penalty for the primary offences is a fine of up to S$500,000 or 10 years' imprisonment, or both upon conviction. For legal persons, it is a fine of up to the higher of S$1,000,000 twice the value of the property involved or services rendered for terrorism financing. A person who abets, conspires or attempts to commit any of the primary offences is subject to the same penalty as if he committed a primary offence.

For the offence of disclosing information (i.e.'' tipping off''), the maximum penalty is a fine of S$250,000 and five years' imprisonment, or both.

The 2019 TSFA amendment introduced a tiered penalty system for the offence of failing to report information about terrorism funding. Individuals who learn the information in the course of their trade, profession, business or employment will attract a fine of up to S$250,000 or five years' imprisonment, or both. This reflects the higher degree of culpability that individuals such as bankers face. Other individuals will attract a fine of up to S$50,000 or five years' imprisonment, or both. Corporations face the highest degree of culpability. Where a terrorism financing offence was committed, they will attract a fine of up to the higher of S$1,000,000 or twice the value of the property involved or services rendered for terrorism financing. Where a terrorism financing offence did not occur, the fine is up to $1,000,000.



Soft laws and knowing your client

For banks, financial institutions, and payment service providers, soft laws consist of notices and guidelines issued by the Monetary Authority of Singapore (MAS). These notices and guidelines are issued by the MAS under the Banking Act (Cap19) and the Monetary Authority of Singapore Act (Cap. 186) and, as their names suggest, the notices consist of rules and guidelines with which financial institutions must comply.

The MAS has issued separate notices and guidelines for different financial institutions in Singapore. This article focuses on the Notice to Banks on Prevention of Money Laundering and Countering the Financing of Terrorism (MAS Notice 626), which was issued on July 2, 2007 and last revised on November 30, 2015 and the Notice to Holders of Money-changers Licence and Remittance Licence (MAS Notice 3001) issued on April 24, 2015 and last revised on January 9, 2019, and the guidelines issued thereunder.

Risk-based approach

Singapore adopts a risk-based approach for the performance of know your customer or customer due diligence (CDD) measures. This means that the licensee can choose the level or extent of checks to be carried out according to the money laundering or terrorist financing risk posed by the customer in question. CDD procedures aim to verify the identity of the customer or beneficiary behind a transaction or account and must be performed through reliable and independent sources. The main concepts of CDD include:

- the identification of a customer by obtaining information about the customer or related persons for customers who are legal persons;
- checking the information obtained for veracity and credibility;
- for legal persons, ascertaining the identity of the natural person acting on the customer's behalf;
- the determination of the existence of any beneficial owners and conducting identification and verification procedures on those beneficial owners;
- the identification of the nature and purpose of the intended business relations/transactions;
- continuing monitoring of the customer's account; and
- periodically review the adequacy of customer information after business relations are established.

In addition to the existing situations where CDD measures have to be performed, banks and various other financial entities licensed by the MAS, including merchant banks, direct life insurers, finance companies, depositories, credit/charge card licensees, money-changers and money remitters (each, a licensee), now have to perform CDD measures for any transaction of a value exceeding S$20,000, or for funds received or effected by domestic or cross-border wire transfer that exceeds S$1,500 for any customer who has not otherwise established business relations with the bank.

Simplified CDD versus enhanced CDD

A bank may perform simplified CDD measures in the event where it is satisfied that the risks of money laundering and terrorism financing are low, and are required to perform enhanced CDD when such risks are high. While what constitutes simplified CDD and enhanced CDD is not defined by the MAS, these must be commensurate with the level of risk based on the risk factors identified by bank, and but they can be explained by the following illustrations:

Illustration one

If the customer is a financial institution which is subject to AML/CFT requirements which are consistent with the standards set by the Financial Action Task Force, the licensee can rely on identification documents which are copies and sent by the customer via facsimile transmission or e-mail. This is an example of simplified CDD.

Illustration two

If the customer is not subject to the Financial Action Task Force requirements and comes from countries known to have money laundering and terrorism activities, the licensee needs to perform enhanced CDD measures by requiring, for example, certified true copies of identification documents or that original documents must be sighted. This is an example of enhanced CDD.

Simplified CDD can be performed on customers who present a low risk of being involved in money laundering or terrorist financing activities, but the MAS notice has made it explicit that simplified CDD shall not be performed where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT measures or where the licensee suspects that money laundering or terrorist financing is involved.

When a licensee performs simplified CDD measures in relation to a customer, it is required to document the details of its risk assessment and the nature of the simplified CDD measures.

On the other hand, circumstances which are to be considered high risk include the following:

- where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the Financial Action Task Force has called for countermeasures, the bank shall treat any business relations with or transactions for any such customer as presenting a higher risk for money laundering or terrorism financing; and
- where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the bank for itself or notified to banks generally by the MAS or other foreign regulatory authorities, the bank shall assess whether any such customer presents a higher risk for money laundering or terrorism financing.

The MAS has issued guidelines to guide financial institutions in their compliance with the requirements of the MAS notice. The nature of CDD checks will depend on the type of customer with which the licensee is undertaking a business dealing, and licensees must adopt the appropriate main concepts in performing the CDD checks. Some of the guidelines are discussed below.

Should financial institutions outsource their AML/CFT functions to external service providers, the MAS in its Guidelines on Outsourcing considers that the outsourcing or risk management or internal control functions to be a material outsourcing arrangement with responsibility remaining with the board and senior management.

Private individuals

For licensees, as of 2019, face-to-face identity verification checks for private individuals are no longer required. However, licensees are obliged to develop policies and procedures to address any specific risks associated with non-face-to-face business transactions or account relationships. They must submit an external auditor or consultant's assessment of the procedures within one year of conducting non-face-to-face business contact. CDD procedures must also be at least as stringent as face-to-face contact CDD measures.

Details of the customer's or beneficial owner's particulars such as full name, including any aliases, existing addresses (residential and corporate if appropriate), date of birth and nationality should be recorded and kept for future references.

Banks should also determine whether the customer or beneficial owner is a politically exposed person (PEP) through reliable database service providers, and take subsequent measures deemed appropriate by the bank. Where face-to-face verification is not possible, it is imperative that banks continue to conduct checks to address any specific risks associated with non-face-to-face business relationships.

Companies

Where the customer is a company, the bank and licensees must identify both the customers and the directors of the company by getting, for example, its certificate of incorporation and other relevant corporate records which show the customer's shareholders and directors.

Similarly, where the customer is a partnership or a limited liability partnership, banks and licensees must, in addition to identifying the customer, identify the partners. For both types of customers, banks and licensees must take steps to identify the persons having control over them.

Customers acting through another party

Where the customer appoints one or more natural persons to act on his behalf (for instance, through an agent, third party or attorney, or the customer is not a natural person) the licensee must take the relevant measures to understand the ownership and control structure of the customer, verify the authority granted to the natural persons and follow up by verifying the identity of the natural persons.

The bank can do so by obtaining appropriate evidence documenting the fact that the customer has appointed the persons to act on its behalf. The bank must also collect specimen signatures for the persons appointed to act for the customer.

Customers of another financial institution

When a bank ("acquiring bank") acquires another financial institution (local or foreign), the acquiring bank shall perform CDD measures on the customers acquired together with the business at the time of acquisition, except where the acquiring bank has acquired at the same time all corresponding customer records and has no doubts or concerns about the credibility of the information so acquired, and where the acquiring bank has conducted due diligence enquiries and is satisfied that the AML/CFT measures previously adopted by the acquired bank are adequate.

For customers who present a higher risk of money laundering and terrorist financing, enhanced CDD measures should be performed. These customers include PEPs, their immediate family members and close associates.

Other categories include customers from or in countries and jurisdictions known to have loose AML/CFT measures as determined by the licensee or notified to the licensee by the MAS, or other foreign regulatory authorities.

Under the MAS notice, a PEP is defined as a natural person who is or has been entrusted with prominent public functions, whether in Singapore or a foreign country, including the roles held by a head of state, head of government, government ministers, senior civil servants, senior judicial or military officials, senior executives of state-owned corporations and senior political party officials, including family members and close associates of the same.

To determine whether a customer is a PEP, the MAS allows licensees to refer to databases of PEPs which have either been compiled commercially or by official authorities. In addition to the requirement to perform the basic identification and verification measures, licensees must:

- have in place and implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP;
- obtain approval from the licensee's senior management to establish or continue business dealings with the customer in question;
- establish by appropriate and reasonable means, the source of wealth or funds of the customer or beneficial owner; and
- conduct enhanced monitoring of the business relations with the customer throughout the business relationship.

This means that licensees must be alert to peculiar fund movements in relation to the customer or beneficial owner and must remain vigilant and monitor the customer's transactions and dealings throughout its professional relationship with the customer.

Identification and verification of identity of beneficial owners

There is a general requirement to ascertain and verify the existence and identities of beneficial owners in relation to a customer, but licensees are not required to do so for the following types of customers:

- an entity listed on the Singapore Exchange;
- an entity listed on a foreign stock exchange that is subject to regulatory disclosure requirements;
- a financial institution supervised by the MAS (with the exception of licensed money changers or holder of a remittance licence unless specifically notified by the MAS);
- a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with AML/CFT requirements consistent with FATF's standards; or
- an investment vehicle where the managers are financial institutions supervised by the MAS or are subject to AML/CFT requirements consistent with FATF's standards if it is incorporated outside of Singapore.

These exemptions are subject to the proviso that should the licensee have doubts about the veracity of the CDD information or suspects that the customer, business relations with, or transactions for the customer may be connected with money laundering or terrorism financing, then the licensee shall inquire into the beneficial ownership.

Performance of CDD by intermediaries

Licensees can rely on an intermediary which is subject to and supervised for compliance by the AML/CFT requirements consistent with the standards of FATF and has adequate measures in place to comply with those requirements. The intermediary must not be one which licensees are precluded by the MAS from relying and it must be willing and able to provide without delay any document obtained by it upon the licensee's request of such documents. Licensees have a positive obligation to document its satisfaction of the intermediary's compliance of the above requirements before using it for CDD measures, and immediately obtain from the intermediary the CDD information obtained by the intermediary on behalf of the licensee. The ultimate responsibility to prevent AML/CFT rests on the licensee and intermediaries cannot be relied upon to perform continuing monitoring.

Virtual currencies

Following the commencement of the Payment Services Act 2019 (PS Act) on January 28, 2020, any service of dealing in, or facilitating the exchange of, digital payment tokens must now be licensed by MAS. Accordingly, any digital payment token service provider, including cryptocurrency dealing or exchange services, must comply with MAS AML/CFT requirements set out in notices. MAS issued the Notice to Holders of Payment Service Licence (Digital Payment Token Service) (MAS Notice PSN02) on December 5, 2019. CDD measures imposed by the notice largely parallel the same AML/CFT requirements imposed on other financial institutions as outlined above, including the same risk-based approach.

Account issuance services, domestic money transfer services, cross-border money transfer services and money-changing services

Previously, money-changing and remittance businesses were regulated under the Money-changing and Remittance Businesses Act (Cap. 187), and the provision of stored value facilities and stored value under the Payment Systems (Oversight) Act 2006. However, these two Acts have been repealed since the commencement of the PS Act, which replaces the regulatory regime for these businesses, and adds a number of additional businesses and activities to its purview.

The newly regulated payment services include:

- domestic money transfer services;
- merchant acquisition services; and
- digital payment token services, including virtual currency as discussed above, Virtual Assets Service Providers (service providers of digital payment tokens that facilitate the use of digital payment tokens for payments and may not possess the moneys or digital payment tokens involved).

Previously regulated activities now fall under broader categories of activities regulated by the PS Act:

- account issuance services;
- e-money issuance services; and
- cross-border money transfer services.

Money-changing services are also regulated by the PS Act, but their definition has not increased in scope.

Beyond digital payment token services, four further types of payment services are obliged to comply with MAS AML/CFT requirements, as set out by the MAS Notice to Holders of Payment Services Licence (Specified Payment Services) (MAS Notice PSN01). These four services are account issuance services, domestic money transfer services, cross-border money transfer services and money-changing services. The AML/CFT requirements largely parallel the same AML/CFT requirements outlined above. In 2021, the definition of cross-border money transfer service was broadened to include facilitating transfers of money between persons in different jurisdictions, where money is not accepted or received by the service provider in Singapore.

Precious metals

Since April 10, 2019, an AML/CFT regulatory regime has been implemented for the precious stones and precious metals dealers through the Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act 2019 (PSPM Act). Beyond being subject to the reporting obligations under the CDSA and the TSFA, PSPM dealers (including intermediaries like auction houses and trading platforms) must register with the Registrar of Regulated Dealers, unless they are already a MAS-regulated financial institution. Regulated dealers must comply with additional regulations in the PSPM Act. This includes implementing CDD measures based on a risk-based approach, alike to financial institutions.

However, the PSPM Act specifically requires regulated dealers to implement CDD measures before entering 'designated transactions', which are cash transactions greater or equivalent to S$20,000. They must also report all entered designated transactions to the STRO, regardless of whether there is suspicion of money laundering or terrorism funding. Further, regulated dealers must keep records of designated transactions, transactions involving CDD measures, and any information obtained through CDD measures.

Notably, unlike the CDSA and TSFA, the PSPM Act has more protections for PSPM dealers to prevent tipping off. It permits regulated dealers to not perform or complete required CDD measures if (1) it is reasonably suspected that the transaction relates to money laundering or terrorism funding; and (2) performing the measures will tip off the customer.

Penalties under the PSPM Act

If a regulated dealer fails to comply with required CDD measures, they are guilty of an offence and liable for a fine of up to S$100,000 upon conviction. If a regulated dealer fails to submit cash transaction reports, they are liable for a fine of up to S$20,000 or two years' imprisonment, or both. If a regulated dealer fails to keep records, they are liable for a fine of up to S$100,000.

Variable capital companies

Variable capital companies (VCC) incorporated under the Variable Capital Companies Act 2018 (VCC Act), in force since January 14, 2020, are also obliged to follow MAS AML/CFT requirements. On January 14, 2020, MAS issued the Notice to Variable Capital Companies on Prevention of Money Laundering and Countering the Financing of Terrorism (MAS Notice VCC-N01) under section 84 of the VCC Act. The notice requires VCCs to perform risk assessment, CDD measures, record keeping, and suspicious transaction reporting by appointing an eligible financial institution (EFI) to conduct the necessary checks and perform the measures. VCCs may rely on the CDD measures already performed by its EFI under two main conditions: the EFI's AML/CFT requirements are consistent with FATF standards, and the member of the VCC is also a customer of its EFI.

Casinos in Singapore

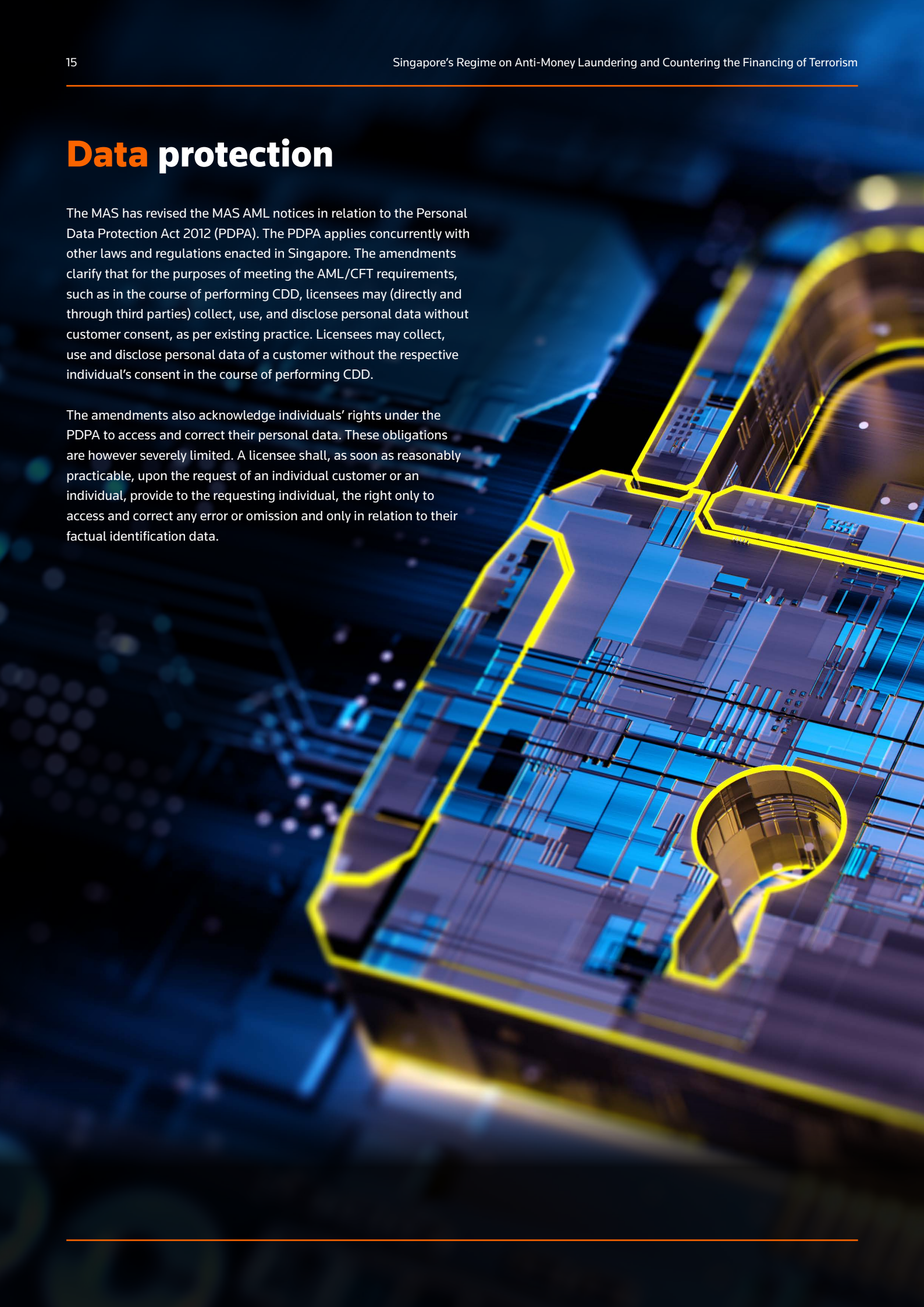
The Casino Control (Prevention of Money Laundering and Terrorism Financing) Regulations 2009 also establishes similar CDD requirements on casinos operating in Singapore and also, in recognition of the fact that casinos are traditional (and the easiest) institutions which may be utilised for money-laundering purposes, obliges casinos operating in Singapore to develop and implement internal policies, procedures and controls to detect and prevent money-laundering and the financing of terrorism activities.

The money laundering and terrorism framework and suspicious transaction reporting framework to be developed by casino operators now extend to all its branch offices.

Data protection

The MAS has revised the MAS AML notices in relation to the Personal Data Protection Act 2012 (PDPA). The PDPA applies concurrently with other laws and regulations enacted in Singapore. The amendments clarify that for the purposes of meeting the AML/CFT requirements, such as in the course of performing CDD, licensees may (directly and through third parties) collect, use, and disclose personal data without customer consent, as per existing practice. Licensees may collect, use and disclose personal data of a customer without the respective individual's consent in the course of performing CDD.

The amendments also acknowledge individuals' rights under the PDPA to access and correct their personal data. These obligations are however severely limited. A licensee shall, as soon as reasonably practicable, upon the request of an individual customer or an individual, provide to the requesting individual, the right only to access and correct any error or omission and only in relation to their factual identification data.



Future developments

FATCA regime changes

The Foreign Account Tax Compliance Act (FATCA) is U.S. legislation that targets non-compliance with tax laws by U.S. persons using overseas accounts. Through FATCA, all financial institutions outside of the U.S. are required to regularly submit information on financial accounts held by U.S. persons to the U.S. Internal Revenue Service (IRS). Since March 18, 2015, Singapore has had an Intergovernmental Agreement (IGA) with the U.S. in force. The IGA allows Singapore financial institutions to comply with FATCA reporting obligations through IRAS.

Currently, non-compliance with FATCA can result in foreign financial institutions (FFI) incurring a potential 30% withholding tax on 'withholdable payments' made to them. This is defined as U.S.-source income, profits and gains. U.S. Proposed Treasury Regulations issued December 18, 2018 removed from the definition any gross proceeds from the sale or other disposition of any property of a type that can produce interest or dividends that are US source fixed, determinable, annual, periodical income. Proposed regulations can be relied on until final regulations are issued, except as otherwise provided.

Furthermore, the same 2018 proposed regulations have again deferred the requirement for FFIs to withhold 'passthru payments' made to recalcitrant account holders and non-FATCA-participating FFIs. The IRS has yet to define 'foreign passthru payments'. FFIs will now not be required to withhold tax on a foreign passthru payment before the date that is two years after the publication of final regulations defining the term foreign passthru payment'. Despite a number of IGAs assisting current compliance with FATCA, the deferral indicates that the IRS remains interested in the withholding providing a possible incentive for the creation and maintenance of more IGAs, and greater FFI FATCA compliance.

Closing thoughts

Singapore continues to place emphasis on a robust regulatory framework given the importance of cross-border and international trade. Singapore's AML and CFT regimes have effectively increased the standard or degree of vigilance which must be observed by banks and licensees, and corresponding with this increase are the costs involved in carrying out these measures. There nevertheless remains a silver lining because Singapore's risk-based approach to CDD means that banks and licensees still have some room to perform CDD or KYC based on their "comfort levels", and financial institutions retain some discretion which can be exercised in its determination of who is high-risk and who is low-risk.

Given rapid technological advancements, the ever-increasing sophistication of money launderers and terrorism financiers and the changing business landscape, such as the number of new casinos which came into operation in 2011, it is inevitable that banks and licensees will have to adjust their respective "comfort levels" and continue to step up on AML/CFT strategies to safeguard the integrity of Singapore's financial markets and ensure that they have sufficient and adequate processes and procedures to prevent themselves from being unwitting participants in money laundering and other dubious activities. Stakeholders, including the legislative authorities themselves, will also have to start to adapt and consider what measures would be appropriate to implement in light of the rising trend of virtual currencies.

About the authors

Bryan Tan

Partner, Pinsent Masons MPillay

Bryan Tan is the Head of TMT practice in Pinsent Masons MPillay Singapore. He is a very experienced practitioner specialising in local and regional aspects of TMT law that merit his excellent market reputation.

Nathanael Lim

Senior Associate, Pinsent Masons MPillay

Nathanael Lim provides specialist legal advice in the technology sector - payment services, e-wallets, e-money, cryptocurrency, software. He also has experience working in a UK Magic Circle law firm and the Supreme Court of Singapore, the highest judicial institution in the country.

About Thomson Reuters Regulatory Intelligence

Our intelligence working for you

Thomson Reuters Regulatory Intelligence is a market leading solution that empowers you to make well-informed decisions to confidently manage regulatory risk, while providing the tools to make proactive decisions and action change within your organisation. It has been developed with a full understanding of your compliance needs – locally and globally, today and in the future.

Schedule a consultation today

THOMSON REUTERS®