

Legal 500

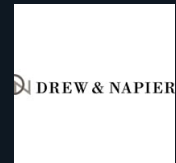
Country Comparative Guides 2026

Singapore

White Collar Crime

Contributor

Drew & Napier



Gary Low

Director and Co-Head of Criminal Law Practice | gary.low@drewnapier.com

Terence Tan

Director | terence.tan@drewnapier.com

Zachary Tong

Senior Associate | zachary.tong@drewnapier.com

This country-specific Q&A provides an overview of white collar crime laws and regulations applicable in Singapore.

For a full list of jurisdictional Q&As visit legal500.com/guides

Singapore: White Collar Crime

1. What are the key financial crime offences applicable to companies and their directors and officers? (E.g. Fraud, money laundering, false accounting, tax evasion, market abuse, corruption, sanctions.) Please explain the governing laws or regulations.

Key financial crime offences include:

(a) various categories of offences under the Penal Code 1871, which contain the majority of criminal offences in Singapore. This includes offences of:

Cheating, under Sections 415 to 420A of the Penal Code. The offence of cheating generally applies to deception and fraud, including where the accused person makes a false statement which induces the victim to part with money or property, or to do things he otherwise would not have done.

Criminal misappropriation and breach of trust, under Sections 403 to 409 of the Penal Code. The offence involves dishonest misappropriation of money or property. Where the accused person is entrusted with property, the offence becomes a more serious criminal breach of trust. Under Section 409 of the Penal Code, a criminal breach of trust by certain categories of persons including directors or key executives of a corporation is liable to be punished more severely.

Forgery and falsification of accounts, under Sections 463 to 477A of the Penal Code. These offences apply where company directors or officers manipulate financial statements, forge auditor signatures on financial statements, or falsify accounts, among other things.

(b) Offences under the Securities and Futures Act 2001 ("SFA"). Offences include false trading and other market manipulation under Sections 197 and 198 of the SFA, as well as insider trading under Sections 218 and 219 of the SFA. For offences under Part 12 of the SFA (relating to market conduct), the company would also be guilty of the offence if the offence was committed with the company's "consent or connivance" and for the benefit of the company. If the company was negligent in failing to prevent or detect a breach under Part 12, the company is also liable to pay a civil penalty.

(c) Offences under the Corruption, Drug Trafficking and

Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA"), which relate to money-laundering. The CDSA criminalises acquiring, possessing, using, concealing or transferring the benefits of crime or any property reasonably suspected of being benefits of crime. A company can also be guilty of CDSA offences through the actions of its directors, employees or agents.

(d) offences under the Prevention of Corruption Act 1960 ("PCA"). The PCA is the primary legislation in Singapore criminalising both public sector and private sector corruption and bribery.

(e) the Income Tax Act 1947 sets out the range of tax-related offences including tax evasion.

(f) the Companies Act 1967 ("CA") sets out the scope of a company and its directors' statutory duties and other obligations, and contains a wide range of offences involving companies and directors.

2. Can corporates be held criminally liable? If yes, how is this determined/attribution?

Corporates can be held criminally liable. Section 2(1) of the Interpretation Act 1965 provides generally that in every written law of Singapore, the word "person" includes any company. Section 11 of the Penal Code defines a "person" as including "any company or association or body of persons, whether incorporated or not".

Most legislation will specify the circumstances in which a company is liable for offences committed by its directors or employees. For example under Part 12 of the SFA, an offence committed by an employee or officer of a corporation, with the consent or connivance of the corporation and for the benefit of the corporation, will equally render the corporation guilty of that offence.

In the context of the CDSA, the High Court in *Abdul Ghani bin Tahy v Public Prosecutor* [2017] 4 SLR 1153 cited *Huckerby v Elliot* [1970] 1 All ER 189 that a director "consents" to the commission of an offence when he is "well aware of what is going on and agrees to it", whereas a director "connives" at the offence if he is "equally well aware of what is going on but his agreement is tacit, not actively encouraging what happens but letting it continue and saying nothing about".

In determining whether criminal liability should be attributed to the company, the focus is on "whether the relevant wrongdoer can be considered to be the directing mind and will of the company in the context of the relevant offending act" and whether the "actions of the employee were in truth reflective of the actions of the company". This is wide enough to capture situations where a company's directors or senior management know that illegal acts are being carried out by a wrongdoer but choose to do nothing (PP v China Railway Tunnel Group Co Ltd (Singapore Branch) [2025] 4 SLR 69).

Similarly, Sections 73(1) and 73(2) of the CDSA provide that the state of mind and conduct respectively of a director, employee or agent of the company can be deemed to be that of the company's if the conduct was engaged in within the scope of the actual or apparent authority of the director, employee or agent.

3. What are the commonly prosecuted offences personally applicable to company directors and officers?

Commonly prosecuted offences personally applicable to company directors and officers include:

- corruption under the PCA
- cheating, forgery and criminal breach of trust under the Penal Code
- negligence as well as making false or misleading statements under the CA
- market manipulation and insider trading under the SFA

4. Who are the lead prosecuting authorities which investigate and prosecute financial crime and what are their responsibilities?

The leading prosecuting authority for all criminal prosecution (whether of financial crime or other crime) is the Attorney-General's Chambers ("AGC"). The AGC is led by the Attorney-General who is concurrently also the Public Prosecutor, who has control and direction of criminal prosecutions and proceedings under the Penal Code and any other written law.

Most criminal prosecutions are conducted by Deputy Public Prosecutors, who are appointed by and act under the authority of the Public Prosecutor, in evaluating evidence and prosecuting offences before the Court.

Investigations of financial crime are conducted by a

variety of different agencies, which often work together. This includes:

- the Singapore Police Force ("SPF"), which is the main police agency in Singapore;
- the Commercial Affairs Department ("CAD"), which is a specialised division of the SPF that investigates financial crime;
- the Corrupt Practices Investigation Bureau ("CPIB"), an independent agency under the Prime Minister's Office which investigates matters of corruption;
- the Monetary Authority of Singapore ("MAS"), which is the central bank and financial regulatory authority and has investigative powers in respect of matters relating to the SFA and Financial Advisers Act 2001 among other things; and
- the Inland Revenue Authority of Singapore, which investigates potential tax offences.

5. Which courts hear cases of financial crime? Are they determined by tribunals, judges or juries?

Offences involving financial crime are typically heard in the State Courts at first instance.

In the State Courts, criminal cases are heard by either the Magistrate's Court (which can hear offences for which the maximum imprisonment does not exceed 5 years) or the District Court (which can hear offences for which the maximum imprisonment does not exceed 10 years).

An appeal from a decision of the Magistrate's Court or the District Court is heard by the General Division of the High Court.

Although the General Division of the High Court has the jurisdiction and power to hear every case, including cases of financial crime, the vast majority of criminal cases in Singapore are heard by the State Courts. The General Division of the High Court typically only hears cases involving the most serious offences including murder, drug trafficking where the death penalty applies, and rape.

On rare occasions, financial crime cases are heard by the General Division of the High Court at first instance (see e.g. Public Prosecutor v Juandi bin Pungot [2022] SGHC 70 involving the mastermind of a large-scale conspiracy to misappropriate gas oil of around S\$128 million, who was eventually sentenced to 29 years' imprisonment).

Under the Singapore judicial system, there are no jury

trials. All trials are heard by judges or judicial officers as finders of fact. Criminal cases are determined by judges and not by tribunals.

6. How do the authorities initiate an investigation? (E.g. Are raids common, are there compulsory document production or evidence taking powers?)

Investigations start when a complaint or report is lodged and/or where the relevant authority has reason to suspect that an offence has been committed. Raids may be conducted where there is a need to preserve evidence or other reasons for urgency. In general, the investigative authorities have document production and evidence taking powers, including to:

- (a) search premises and seize evidence;
- (b) examine witnesses and take statements from them;
- (c) order the production of documents, including customer information from a bank;
- (d) access computers to search any data and make copies of any data; and
- (e) arrest suspects.

The exact scope of powers depend on the agency involved and the offence under investigation.

Failure to comply with such orders or obstructing the investigative authorities in their lawful exercise of powers also constitutes a criminal offence.

7. What powers do the authorities have to conduct interviews?

Under Section 21 of the CPC, a police officer may issue a written order requiring anyone within the limits of Singapore, who appears to be acquainted with any of the facts and circumstances of the case, to attend before the police officer. If the person fails to attend as required, the police officer may report the matter to a Magistrate who may then issue a warrant ordering the person to attend.

Under Section 22 of the CPC, the police officer may examine orally any person who appears to be acquainted with the facts of the case, and record a statement in writing or in the form of an audio-visual recording.

8. What rights do interviewees have regarding the interview process? (E.g. Is there a right to be represented by a lawyer at an interview? Is there an absolute or qualified right to silence? Is there a right to pre-interview disclosure? Are interviews recorded or transcribed?)

There is no right to be represented by a lawyer during an interview by the police or other authorities. There is no legal rule requiring the police to let counsel be present during interviews with the accused, while investigations are carried out (*Muhammad bin Kadar v Public Prosecutor* [2011] 3 SLR 1205 at [57]).

Under Article 9(3) of the Constitution of the Republic of Singapore, an arrested person is allowed to consult and be defended by a legal practitioner of his choice. However, this right only arises within a reasonable time after arrest, the rationale being to afford the police a degree of latitude in carrying out their investigations (*James Raj s/o Arokiasamy v Public Prosecutor* [2014] 2 SLR 307 at [5]).

There is only a limited right to silence under the CPC 2010. Under Section 22(2) of the CPC, a person giving a statement is bound to state truly what the person knows of the facts and circumstances of the case, except that the person need not say anything that might expose the person to a criminal charge, penalty, or forfeiture. However, failing to mention facts in statements to the police may be detrimental if the accused person subsequently wants to rely on those facts in his defence. Under Section 261 of the CPC, the Court may draw the necessary inferences against the accused from a failure to mention his defence in his investigative statements.

For statements recorded by the CPIB under the PCA, there is no right to silence. Section 27 of the PCA requires that every person required to give information to the CPIB is legally bound to give that information.

There is generally no right for an interviewee (whether as a suspect or a witness) to pre-interview disclosure. As a matter of discretion, a witness (meaning a person assisting with investigations who is not suspected of crime) may be provided with some context about the scope of investigations and what they may be questioned about during the interview.

Under Section 22(3) of the CPC 2010, statements made are recorded either in writing or in the form of an audio-visual recording. In practice, statements are usually typed out by the recording officer during the interview or hand-written and subsequently transcribed into type-written

form before the final statement is signed by the interviewee.

9. Do some or all the laws or regulations governing financial crime have extraterritorial effect so as to catch conduct of nationals or companies operating overseas?

The starting position is that legislation in Singapore does not have extraterritorial effect, unless expressly provided for (Public Prosecutor v Muhammad Farid bin Sudi [2017] SGHC 228 at [64]).

Some of Singapore's laws and regulations governing financial crime are expressly stated to have extraterritorial effect. Examples relevant to financial crime offences include the following:

PCA: Section 37 of the PCA provides that the PCA applies extraterritorially to corruption offences committed by Singapore citizens both within and outside Singapore.

Penal Code: Public servants who are citizens or permanent residents of Singapore can be prosecuted for offences they commit outside Singapore when acting or purporting to act in the course of their employment (see Section 4 of the Penal Code).

Under Section 4B of the Penal Code, certain specified offences can also be prosecuted in Singapore where a physical element of the offence occurs in Singapore. This includes offences of dishonest misappropriation, criminal breach of trust, cheating, forgery, and other fraud-related offences among other things.

10. Do the authorities commonly cooperate with foreign authorities? If so, under what arrangements?

The Singapore authorities regularly cooperate with foreign authorities through various forms of mutual legal assistance.

The arrangements made are typically on a reciprocal basis by way of bilateral treaties or multilateral conventions between countries. In Singapore, relevant legislation facilitating mutual legal assistance include:

- (a) the Mutual Assistance in Criminal Matters Act 2000;
- (b) the Extradition Act 1968;
- (c) the Terrorism (Suppression of Financing) Act 2002; and

(d) the Terrorism (Suppression of Bombings) Act 2007.

Amongst other things, the Attorney-General may request the assistance of foreign authorities to obtain evidence, arrange for potential witnesses to attend in Singapore, enforce Singapore confiscation orders, and locate and identify persons outside of Singapore. Foreign authorities may similarly seek such assistance from Singapore.

11. What are the rules regarding legal professional privilege? What, if any, material is protected from production or seizure by financial crime authorities?

Legal professional privilege in Singapore comprises both legal advice privilege and litigation privilege (see e.g. Sections 128 and 131 of the Evidence Act 1893).

Legal advice privilege provides that confidential communications made between a client and their lawyer for the purpose of seeking legal advice are privileged and may not be disclosed without the consent of the client (Skandinaviska Enskilda Banken AB (Publ), Singapore Branch v Asia Pacific Breweries (Singapore) Pte Ltd [2007] 2 SLR(R) 367 ("Skandinaviska") at [43]).

Litigation privilege applies to every communication, whether confidential or otherwise so long as it is for the purpose of litigation (Skandinaviska at [44]). The party seeking privilege must show that there was a reasonable prospect of litigation and that the dominant purpose of the existence of the documents must have been for the purpose of litigation.

Communications made in furtherance of an illegal purpose are not protected from disclosure by legal professional privilege under Section 128(2) of the Evidence Act 1893.

The broad investigative powers of seizure and document production under the CPC and the PCA do not expressly prohibit or protect privileged material from seizure by the authorities.

The authorities may be able to seize privileged information given the breadth of investigative powers available. However, they would not be able to freely use such privileged information. The High Court in Ravi s/o Madasamy v Attorney-General [2021] 4 SLR 956 set out the procedure to be followed when privileged information has been seized (at [83]-[89]).

(a) the AGC should conduct a review of the seized materials for legal professional privilege. The review

should be conducted by a team of AGC officers (the "AGC privilege team") who are not involved in the investigation. This could exclude officers from the AGC's Crime Division or the AGC's Civil Division depending on the circumstances in which the claim of privilege arises;

(b) the lawyer asserting privilege should identify what specific documents or files are protected by legal privilege. If he cannot remember which specific documents are privileged, he can inform the AGC and the AGC privilege team should provide supervised access;

(c) the AGC privilege team may accept a claim of legal professional privilege at face value, or they may review the identified materials to determine if they agree that the identified materials are privileged;

(d) If the documents are privileged, they should be returned if possible. If the seized documents are in softcopy and cannot be feasibly returned, they should be isolated or quarantined such that subsequent investigators or prosecuting officers will not chance upon the privileged materials;

(e) If the documents are not privileged, the AGC privilege team should inform the lawyer, who can consult with the affected client for the client to decide whether to insist on his claim to privilege or waive privilege;

(f) If the affected client waives privilege, the issue is resolved. If the affected client insists on his claim to privilege, he can either file an application under Order 53 of the Rules of Court 2014 (now under Order 24 of the Rules of Court 2021) for leave for a prohibiting order, or object to the admission of the privileged material in question into evidence on the grounds of legal professional privilege; and

(g) If an application is filed and there are judicial review proceedings, the identified materials should not be handed over to the investigating authority and the prosecution team until after the court challenge is decided.

The Prosecution may also rely on litigation privilege, where the Prosecution can show that the communications are made at a time when there was a reasonable prospect of litigation, and are made for the dominant purpose of litigation (*Public Prosecutor v Soh Chee Wen* [2020] 3 SLR 1435 at [11], [14] and [15]).

Only some specific legislation expressly provides that privileged material is protected from production or seizure. For example, Section 36 of the CDSA provides that the Court may order production of documents in relation to CDSA investigations into drug dealing or

criminal conduct. One of the required conditions is that there are reasonable grounds to believe that the material is of substantial value and does not consist of items subject to legal privilege.

Under Section 105L(5) of the Income Tax Act 1947, information subject to legal privilege is carved out from the general obligation to furnish information to the Comptroller of Income Tax. Under Section 65B(2) of the Income Tax Act 1947 relating to the Comptroller's power to obtain information, information subject to legal privilege is similarly excluded from production or disclosure.

12. What rights do companies and individuals have in relation to privacy or data protection in the context of a financial crime investigation?

Singapore has data privacy and protection rules under the Personal Data Protection Act 2012 ("PDPA"). However, use of data for criminal investigations is generally permitted.

Paragraph 3 of Part 3 of the First Schedule to the PDPA provides that the collection, use and disclosure of personal data without consent is allowed where it is necessary for any investigations or proceedings.

The banking secrecy obligation under Section 47(1) of the Banking Act 1970 is also expressly subject to disclosure in compliance with requests to provide information for the purpose of investigation or prosecution, in relation to alleged offences under any written law, among other things.

13. Is there a doctrine of successor criminal liability? For instance in mergers and acquisitions?

The starting position is that each company is a separate legal entity and that a company is therefore not criminally responsible for the conduct of another. However, the individuals involved in the acquired company can still be held to account as their criminal liability is not affected by the merger and/or acquisition.

Where a company and its directors have been involved in criminal activity, a merger will not absolve the directors of their individual criminal responsibility.

14. What factors must prosecuting authorities

consider when deciding whether to charge?

The AGC does not publish guidelines on its exercise of prosecutorial discretion, including the factors considered in deciding whether to charge. Nevertheless, the Prosecution will consider, among other things, the sufficiency of evidence as well as the consideration of what is in the public interest.

There are no specific factors enshrined in legislation that the prosecuting authorities must consider.

In general, factors considered by the AGC in its exercise of prosecutorial discretion include:

- (a) whether the evidence supports a reasonable prospect of conviction;
- (b) whether the public interest is supported by prosecuting the suspect;
- (c) the nature, severity and scope of the offences committed;
- (d) the harm caused by the offence, including whether restitution has been made;
- (e) the character of the offence, including whether it offends the values expected by the public;
- (f) public interest or public policy considerations; and
- (g) offender-specific factors, including young age, prior convictions, cooperation with the authorities or contrition.

15. What is the evidential standard required to secure conviction?

The Prosecution must prove all the elements of each offence beyond a reasonable doubt.

16. Is there a statute of limitations for criminal matters? If so, are there any exceptions?

There is no statute of limitations for the prosecution of criminal matters. Nevertheless, where there has been an inordinate delay in prosecution, this may be a factor considered by the Court in determining the appropriate sentence.

17. Are there any mechanisms commonly used to resolve financial crime issues falling short of a

prosecution? (E.g. Deferred prosecution agreements, non-prosecution agreements, civil recovery orders, etc.) If yes, what factors are relevant and what approvals are required by the court?

Before charge

Even where the Prosecution takes the view that an offence has been committed, they may choose to issue a warning to the suspect instead of pursuing criminal charges. This is in the Prosecution's exercise of their discretion, and could be for a variety of reasons including youth of the offender, other mitigating circumstances, or where the offence is comparatively minor.

Warnings may be unconditional (generally known as a stern warning) or conditional (stipulating for example that if the suspect commits any other offences within a period of time, the Prosecution will prosecute the suspect for the earlier offence).

The Prosecution's decision not to bring a charge is not subject to the Court's approval.

After charge

Even after a person has been charged in Court, at any stage of proceedings before the accused person is sentenced, the Prosecution may choose to inform the Court that they will not further prosecute the accused person. In these circumstances, the proceedings must be stayed and the accused must be discharged. This is also not subject to the Court's approval.

Composition of offences

Some offences may be compounded. Compounding an offence involves payment of a sum of money, whether to the victim or to the state depending on the type of offence, in lieu of criminal prosecution.

Under Sections 241 and 242 of the CPC 2010, composition of an offence means that no further proceedings are to be taken any further. Where a charge has already been brought, composition has the effect of an acquittal and the Court must order a discharge amounting to an acquittal.

Deferred Prosecution Agreements ("DPAs")

A company, partnership, limited liability partnership or unincorporated association may enter into a DPA with the Public Prosecutor. DPAs do not apply to individuals.

Under a DPA, the Public Prosecutor would agree not to prosecute the entity in criminal proceedings, in exchange for the entity agreeing to certain specified conditions under the CPC 2010, including payment of a financial penalty, compensating victims, disgorging profits from the offence, implementing compliance programmes, or cooperating in investigations into other offences arising from the same facts, among other possible requirements.

DPA's only apply to certain types of offences listed in the Sixth Schedule to the CPC 2010, including falsification of accounts under Section 477A of the Penal Code, corruption under Sections 5 and 6 of the PCA, or various money laundering offences under the CDSA.

DPA's are subject to approval by the General Division of the High Court, and are heard by the High Court in private. The DPA is subject to the High Court granting a declaration that the DPA is in the interests of justice and that its terms are fair, reasonable and proportionate.

18. Is there a mechanism for plea bargaining?

The practice of plea bargaining is common in Singapore and usually takes place after an accused is charged in Court. The accused person or his lawyers may write letters of representation to the AGC to urge the Prosecution not to initiate criminal proceedings, or to withdraw, amend or reduce the charge(s). Such representations highlight mitigating factors or other circumstances to urge the Prosecution to reconsider their exercise of prosecutorial discretion. The Prosecution may make a plead guilty ("PG") offer to the accused. Under a PG offer, the Prosecution may agree to proceed only on some of the charges with the remainder to be taken into consideration for the purpose of sentencing, or may agree to proceed on charges of reduced severity, if the accused person decides to plead guilty.

Another available process are Criminal Case Management System discussions. These are private and without prejudice meetings to enable the Defence and the Prosecution to discuss the case, narrow the issues in dispute, and potentially reach an earlier resolution of the criminal matter.

Unlike plea bargaining in other jurisdictions, the sentence to be imposed remains solely within the Court's discretion regardless of what has been agreed between the Prosecution and the Defence through plea-bargaining. The Court may impose a sentence different from what was agreed between the parties.

19. Is there any obligation to disclose discovered misconduct to prosecuting authorities, or any benefit to making a voluntary disclosure? Is there an established route or official guidance for making such disclosures?

Certain categories of offences must be disclosed and reported to the police or other relevant authorities.

For example, Section 424 of the CPC provides that in the absence of a reasonable excuse, certain specified offences under the Penal Code (most of which involve violence or robbery) must be reported. The failure to report the matter would be an offence.

Section 45 of the CDSA also provides that a person who knows or has reasonable grounds to suspect that any property represents the proceeds of, was used in connection with, or is intended to be used in connection with any act which may constitute criminal conduct, must file a suspicious transaction report as soon as reasonably practicable. Breach of this requirement also constitutes an offence.

The main benefit of voluntary disclosure is to show cooperation and contrition for the offence having happened, which may constitute a mitigating factor in negotiations with the Prosecution in plea bargaining to seek withdrawal or reduction of charges, or for the Court's consideration in determining the appropriate sentence.

There is official guidance in respect of filing suspicious transaction reports, cash movement reports, as well as cash transaction reports. The exact guidance depends on the entity in question and the type of transaction being reported (see e.g. <https://www.police.gov.sg/Advisories/Commercial-Crime/s/Suspicious-Transaction-Reporting-Office/Suspicious-Transaction-Reporting>).

20. What rules or guidelines determine sentencing? Are there any leniency or discount policies? If so, how are these applied?

In general the Court will consider:

- any sentencing benchmarks or frameworks set out by the Court in precedent cases;
- offence-specific factors, including harm caused by the offence and the culpability of the offender. For financial crimes, this includes but is not limited to the amount or value

involved in the offence, involvement of a syndicate and/or transnational element, degree of planning and premeditation, level of sophistication, duration of offending, and extent of the offender's abuse of position and breach of trust, among other things (see e.g. *Takaaki Masui v Public Prosecutor* [2021] 4 SLR 160 at [239]);

- if the offence is hard to detect or if the offender has taken steps to hide the offence or hide his involvement, this is usually an aggravating factor; and
- in the company context, if the accused person holds an important position and his offences reflect a significant abuse of trust, this is a further aggravating factor.

The Court will also take into account any mitigating factors. This includes a plea of guilt, remorse, and the extent to which restitution has been made.

Most sentencing is determined by reference to case law guidance on general sentencing principles, frameworks for specific offences, as well as offence-specific or offender-specific factors. The factors to consider vary case by case, depending on the offence.

In respect of pleas of guilt, the Sentencing Advisory Panel has published a set of Guidelines for the Reduction of Sentences for Guilty Pleas (the "Sentencing Guidelines") which provides guidance on the ranges of reduction in sentence that a court may consider granting based on when an accused person pleads guilty. The Sentencing Guidelines took effect from 1 October 2023.

The Sentencing Advisory Panel comprises among other persons, Judges of the Court of Appeal, the Appellate Division of the High Court, the General Division of the High Court, and persons from the Ministry of Law.

These guidelines are technically not binding and the Court may consider whether or not to adopt the guidelines and how they should be applied. However as a general practice, the Court currently appears to expressly consider and place weight on the Sentencing Guidelines for recently prosecuted cases.

The stages for pleas of guilt under the Sentencing Guidelines generally operate as follows:

(a) Stage 1: an accused person who pleads guilty to a charge from the first mention until 12 weeks after the hearing when the prosecution informs the court and the accused person that the case is ready for the plea to be taken is entitled to a maximum reduction of 30%;

(b) Stage 2: an accused person who pleads guilty after Stage 1 but before the court first gives directions for the filing of the Case for the Prosecution (for cases subject to the Criminal Case Disclosure procedures) or when the court first fixes trial dates (for cases not subject to the Criminal Case Disclosure procedures) is entitled to a maximum reduction of 20%;

(c) Stage 3: an accused person who pleads guilty after Stage 2 but before the first day of trial is entitled to a maximum reduction of 10%; and

(d) Stage 4: an accused person who pleads guilty on or after the first day of trial is entitled to a maximum reduction of 5%.

These reductions are of general application. One exception is where it would be contrary to the public interest to apply the guidelines, in which case the Court may apply a reduction which is just and proportionate instead.

Under the Sentencing Guidelines, the recommended approach is for the Court to first determine the sentence that would have been imposed if the accused person was convicted after trial. Next, the Court determines the applicable stage of proceeds at which the accused person pleaded guilty, as explained above. Finally, the Court applies the reduction to the sentence, which generally should not exceed the maximum reduction explained above.

For cases involving multiple charges, the total sentence is still to be determined based on prevailing sentencing principles. This would include general principles of proportionality and totality.

Under these Sentencing Guidelines, the strength of the evidence should not be taken into account when determining the level of reduction in sentence.

On 21 August 2024, the Sentencing Advisory Panel also published Guidelines for Scams-Related Offences which provide guidelines on how certain specific CDSA and Computer Misuse Act 1993 ("CMA") offences should be sentenced. These guidelines are similarly not binding on the Court. The guidelines took effect immediately and include recommended starting sentences as well as the offender- and offence-specific factors to be considered when adjusting the starting sentence.

The stipulated offences are:

(a) Sections 51(1), 51(1A) and 55A(1) of the CDSA which relate to handing over control of a bank account to a third-party;

(b) Sections 8A and 8B of the CMA, which relate to unlawful disclosure of Singpass credentials; and

(c) Section 420 of the Penal Code for cheating, where the deception is communicated over the phone or online through a communications platform

21. How are compliance procedures evaluated by the prosecuting authorities and how can businesses best protect themselves?

The existence of sufficient compliance procedures help support the argument that the offence was committed by a rogue company officer, and therefore should not be attributed to the company. This involves the principles of attribution in the criminal law context (see question 2 above).

For example, Section 236C of the SFA provides that a corporation which fails to prevent contravention of market misconduct under Part 12, where the contravention is for the corporation's benefit and attributable to the corporation's negligence, has committed an offence and would be liable to a civil penalty.

Section 236C(7) explicitly provides that in determining whether the contravention is due to the corporation's negligence, the Court is to take into account whether the corporation has established adequate policies and procedures to prevent and detect such market misconduct, and whether the corporation has consistently enforced these policies and procedures.

22. What penalties do the courts typically impose on individuals and corporates in relation to the key offences listed at Q1?

For individuals, financial crime offences are often punished with terms of imprisonment unless the amounts involved are very low or there are strong mitigating factors involved.

For corporate entities, the usual punishment is a fine.

In cases involving corruption, the Court may also impose penalties on the recipients of bribes to cause them to disgorge the full amount of the bribes received.

23. What rights of appeal are there?

Persons convicted at first instance in the State Courts may appeal to the General Division of the High Court.

Persons convicted at first instance by the General Division of the High Court may appeal to the Court of Appeal.

There is only one tier of appeal, such that a person convicted at first instance in the State Courts does not have an automatic right to further appeal to the Court of Appeal if his appeal is dismissed by the General Division of the High Court.

A person who claims trial and is convicted after trial may appeal against both the conviction and sentence imposed. However, a person who pleads guilty is generally not entitled to challenge his conviction and may only appeal against the sentence imposed.

The Prosecution is entitled to appeal against either acquittal or the sentence imposed.

The sentence imposed would only be overturned on appeal if shown to be either manifestly inadequate or manifestly excessive.

24. How active are the authorities in tackling financial crime?

The Singapore authorities take active and regular steps to tackle all financial crime, including corruption. Scams of various types are a current problem.

On 22 March 2022, the CAD operationalised the Anti-Scam Command ("ASCom") which comprises the Anti-Scam Centre ("ASC") and three Anti-Scam Investigative Branches, and oversees the Scam Strike Teams situated within each of the seven Police Land Divisions. Various institutions including DBS, HSBC, SCB, UOB, CIMB, OCBC, and GovTech have co-located their staff within the ASCom to enhance real-time coordination with the police in investigation, tracing funds, and swift freezing of bank accounts. This co-location initiative was also expanded to include Carousell and Shopee staff in 2024, and GXS Bank in March 2025. In the first half of 2025, the ASCom froze more than 8,600 bank accounts and recovered more than S\$39.7 million. Another S\$17 million in cryptocurrency was recovered, making up a total recovery of S\$56.7 million.

The ASC also works closely with local telecommunication companies, social media platforms and online marketplaces to terminate mobile lines, suspicious accounts and advertisements involving suspected scams.

The ASC also operationalised the Crypto Tracing Team in March 2025 and established partnerships with over 10

stakeholders, including digital payment token service providers, major payment institutions, and stablecoin issuers. This allows the authorities to better trace, freeze, and recover scam-tainted virtual assets in light of the emerging threat of scam proceeds being rapidly dissipated via virtual assets.

25. In the last 5 years, have you seen any trends or focus on particular types of offences, sectors and/or industries?

The total number of scam cases has increased year on year from 15,651 cases in 2020 to 51,501 cases in 2024. The total amount lost to all scams has similarly increased from S\$265.7 million in 2020 to S\$1.1 billion in 2024. This was a substantial increase of over 70% in total amount lost compared to 2023. Nevertheless, the net scam losses was about S\$930 million because ASCom successfully recovered more than S\$182 million of scam losses. Cryptocurrency losses formed a larger percentage of scam losses, increasing from about 6.8% to about 24.3% of total scam losses from 2023 to 2024.

Other notable offences include criminal breach of trust, corruption, and accounting and financial statement fraud.

The latest MAS Enforcement Report published on 14 April 2025 also noted that the key areas of focus for MAS include:

1. Investigating market abuse (e.g. insider trading, false trading, and disclosure-related breaches);
2. Investigating financial services misconduct (e.g. mis-selling of financial products, breaches of business conduct rules, and serious unfitness and impropriety);
3. Investigating money laundering-related control breaches and enforcing AML/CFT controls; and
4. Building enforcement capabilities in the digital asset ecosystem.

Anti-corruption continues to be a major focus of law enforcement in Singapore, with the CPIB often pursuing investigations in line with Singapore's zero-tolerance approach to corruption. This includes both private sector and public sector corruption.

26. Have there been any landmark or notable cases, investigations or developments in the past year?

Notable cases

As of October 2025, two former bank relationship managers (Wang Qiming and Liu Kai) and a driver (Liew Yik Kit) linked to the S\$3 billion AML case have been charged and convicted:

- Wang Qiming was sentenced to 24 months' imprisonment for various offences of forgery, money laundering, and obstruction of justice under the Penal Code and CDSA;
- Liu Kai was sentenced to four months' imprisonment for using an offence of using a forged document as a genuine document under the Penal Code; and
- Liew Yik Kit was sentenced to three months' imprisonment for offences of lying to the police and obstruction of justice under the Penal Code.

On 14 October 2025, the United States Department of Justice indicted Chen Zhi, the alleged founder and chairman of Prince Holding Group, for wire fraud conspiracy, money laundering conspiracy, and for directing the operation of forced-labour scam compounds in Cambodia. On 30 October 2025, the SPF mounted an enforcement operation at multiple locations island-wide against Chen Zhi and his associates in relation to offences of money laundering and forgery, based on the information received from the Suspicious Transaction Reporting Office as well as investigations with member agencies of the Anti-Money Laundering Case Coordination and Collaboration Network. The SPF have since seized and issued prohibition of disposal orders against six properties and various financial assets with a total estimated value of more than S\$150 million. Other assets, including a yacht, 11 cars and multiple bottles of liquor were also subjected to prohibition of disposal orders. SPF investigations are still ongoing.

Protection from Scams Act 2025

On 1 July 2025, the Protection from Scams Act 2025 came into force. Under this act, the SPF are able to issue restriction orders to a bank to restrict money transfers, ATM facilities, and credit facilities of an individual where the SPF have a reasonable belief that (1) the individual will execute a transfer, withdrawal, or draw down for the purposes of benefitting a scammer; and (2) the restriction order is necessary for the protection of the individual.

This Act empowers the SPF to intervene to prevent further losses, in cases where victims remain unconvinced that they are being scammed. As of August 2025, two restriction orders have been issued by the SPF

to banks to restrict the banking transactions of two individuals.

In passing the bill, Parliament noted that restriction orders will only be issued as a last resort, if all other efforts to convince the individual has failed. There are several other safeguards including that restriction orders are limited to a maximum of 30 days at the outset, the SPF may vary the restriction order temporarily to allow the individual to have access to the money in his or her bank accounts, and there is an appeal process to allow individuals to appeal against the issuance of a restriction order. The Protection from Scams Act 2025 therefore aims to strike a balance between protecting an individual from further harm and not duly inconveniencing the individual.

Criminal Law (Miscellaneous Amendments) Act 2025

On 30 December 2025, various legislative amendments under the Criminal Law (Miscellaneous Amendments) Act 2025 came into force. The Act introduced various legislative amendments, including the introduction of caning for scams and scams-related offences.

Notably, scammers and members/recruiters of scam syndicates will face mandatory caning of at least 6 strokes and up to a maximum of 24 strokes. Under certain circumstances, scam mules who enable scammers by laundering scam proceeds, providing SIM cards, and/or providing Singpass credentials will also face discretionary caning of up to 12 strokes.

Funds Recovery Operations & Networks Team, Inspiring Effective Resolution Plus (FRONTIER+)

FRONTIER+ is a cross-border collaboration platform established on 21 October 2024. At the time of its formalisation, FRONTIER+ involved the anti-scam units of six jurisdictions (Singapore, Hong Kong SAR, Thailand, the Republic of Korea, the Republic of Maldives, and Malaysia). In 2025, a further five jurisdictions (Australia, Macao SAR, Canada, Indonesia, and Brunei) joined the network.

Singapore's ASCom conducted the first Operation FRONTIER+ with Malaysia's National Scam Response Centre and several of Malaysia's government agencies between February and March 2025. Over 300 persons were arrested, and more than S\$2 million was recovered.

Singapore's ASCom also conducted one of the biggest anti-scam operations with the anti-scam units of six other overseas law enforcement agencies (Hong Kong SAR, Macau SAR, Malaysia, Thailand, the Republic of Korea, and the Republic of Maldives) under FRONTIER+

between May and June 2025. This operation involved over 2,780 law enforcement officers and resulted in the freezing of over 32,600 bank accounts, recovery of more than S\$26.2 million, and the arrest of over 1,800 persons.

27. Are there any pending or proposed changes to the legal, regulatory and/or enforcement framework?

On 17 September 2025, it was announced that the SPF, MAS, Infocomm Media Development Authority, and Government Technology Agency of Singapore are working with industry partners to implement new measures against scam mules. Under the new facility restriction framework, scam mules may face various restrictions including:

- restrictions on access to banking services that could be used to move scam monies (i.e. digital banking services, card-based transactions, and ATM services);
- restrictions on access to telecommunications, such as prohibitions on subscription of new mobile lines; and
- restrictions on access to Singpass/Corppass services, such as prohibiting access to existing Corppass accounts or the use of Singpass accounts to register for services that are at higher risk of being exploited for scams (e.g. bank account opening).

These restrictions are important because scammers rely heavily on local facilities to carry out the scams. Internet banking and PayNow are the primary methods for moving scam monies, and scammers make use of local facilities sold to them by mules to electronically move scam monies. Local phone lines are also coveted by scammers, given that Singaporeans are more suspicious of calls or texts from foreign phone numbers.

The restrictions may be imposed on persons who have been warned, issued with composition sums, prosecuted, or convicted of mule-related offences (e.g. Sections 50, 51, 43, 54, 55, and 55A CDSA) or persons under investigation for mule-related offences and are assessed to be at risk of further facilitating scams (e.g. individuals who persist in applying for new facilities to facilitate scams while being investigated or those whose conduct indicates an intent to profit from providing such facilities to scam syndicates).

The facility restriction framework is being implemented in phases with effect from October 2025, starting with restrictions on access to banking services and prohibition

on subscription of new mobile lines.

28. Are there any gaps or areas for improvement in the financial crime legal framework?

Under the current legislative framework, each financial institution is required to take steps to prevent money-laundering. However, financial institutions are unable to share information with each other, which may result in criminals abusing this information asymmetry to hide

illicit funds.

In April 2024, MAS launched a secure electronic information sharing platform named COSMIC to allow participating financial institutions to share information on customers who exhibit potential financial crime concerns. The initial phase of COSMIC involves six Singapore banks (DBS, OCBC, UOB, SCB, Citibank, and HSBC), during which all sharing will be on a voluntary basis for a period of two years.

Contributors

Gary Low

Director and Co-Head of Criminal Law Practice

gary.low@drewnapier.com



Terence Tan

Director

terence.tan@drewnapier.com



Zachary Tong

Senior Associate

zachary.tong@drewnapier.com