THE LEGAL HERALD

ISSUE 02 | 2024

In this issue...

LH AG ADVOCATES AND SOLICITORS

@LHAG www.lh-ag.com @lhagmy

ABOUT US

Lee Hishammuddin Allen & Gledhill is one of the largest law firms in Malaysia and has been providing personalised legal representation since 1902. While our size and long heritage assure clients that they are in capable hands, we have also proven to be adept and dynamic partners in their affairs. We think outside the box and provide novel solutions that are different from others.

Our deals experience includes major corporate and commercial transactions associated with or materially impacting social, economic, and financial developments in Malaysia. We have also acted on some of the most difficult and complex cases, and our decisions have significantly shaped the country's laws. Our clients range from government authorities and companies to conglomerates, financial institutions, multinational corporations, as well as small and medium-sized enterprises (SMEs), start-ups, and private individuals.

We have advised or led on both contentious and non-contentious matters in jurisdictions outside Malaysia, often requiring foreign law advice. As the only firm in the country to be selected as a member of Multilaw and Interlaw, each of which is an international network of prominent independent law firms, we have access to over 8,000 lawyers in more than 150 cities worldwide.

Consistently ranked as one of the leading law firms in the country by prestigious industry publications such as Chambers Asia-Pacific, The Legal 500 Asia-Pacific, Benchmark Litigation Asia-Pacific, Asialaw Profiles, Asian Legal Business, and IFLR1000.

CONTENTS

KDN PP 12853/07/2012 (030901)

APPLE'S ANTITRUST SAGA

by Hoi Jack S'ng & Aida Faralyana Binti Azlan

Apple fined by the European Commission over its in-app purchases system after a complaint by Spotify.

On 4 March 2024, the European Commission (**Commission**) fined Apple over €1.8 billion for abusing its dominant position in the market for the distribution of music streaming apps to iPhone and iPad users (**iOS users**) through its App Store. In particular, the Commission found that Apple applied restrictions on app developers, preventing them from informing iOS users of alternative and cheaper music subscription services available outside of the app (i.e., anti-steering provisions).[1]

Background

The investigation by the Commission began in June 2020, after a complaint from Spotify, a music streaming provider and competitor of Apple Music. Spotify raised issues with two rules found in Apple's license agreements with developers and the associated App Store Review Guidelines, and their impact on competition for music streaming services.[2]

Article 101 of the Treaty on the Functioning of the European Union (**TFEU**) prohibits anticompetitive agreements and decisions of associations of undertakings that prevent, restrict, or distort competition within the EU's Single Market, whereas Article 102 of TFEU prohibits the abuse of a dominant position.

Article 102(a) of the TFEU provides that any abuse by one or more undertakings of a dominant position within the internal market, or in a substantial part of it, shall be prohibited as incompatible with the internal market in so far as it may affect trade between Member States. Such abuse may, in particular, consist of (a) directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions.

Infringement

The two rules imposed by Apple in its license agreement with music streaming app developers are as follows[3]:

a. The mandatory use of Apple's proprietary in-app purchase system (**IAP**) for the distribution of paid digital content. Apple charges app developers a 30% commission fee on all subscriptions bought through the mandatory IAP. The Commission's investigation showed that most streaming providers passed this fee on to end users by raising prices; and

b. "Anti-steering provisions", which limit the

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161
[2] ibid
[3] https://ec.europa.eu/commission/presscorner/detail/es/ip_21_2061

ability of app developers to inform users of alternative purchasing possibilities outside of apps. While Apple allows users to use music subscriptions purchased elsewhere, its rules prevent developers from informing users about alternative and cheaper music subscription services available outside the app.[4]

The Commission concluded that Apple's anti-steering provisions amount to unfair trading conditions, in breach of Article 102(a) of the TFEU. These anti-steering provisions are neither necessary nor proportionate for the protection of Apple's commercial interests and negatively affect the interests of iOS users, who cannot make informed and effective decisions on where and how to purchase music streaming subscriptions for use on their device as information is withheld from them.[5]

In addition to the fine, the Commission has also ordered Apple to remove the anti-steering provisions. This order echoes a requirement under a new EU rule – the Digital Markets Act (**DMA**), which came into force on 7 March 2024.[6]

It is important to note that market dominance is not illegal under the TFEU. However, dominant companies must not abuse their powerful market position by restricting competition.

Following the Commission's decision, Apple has stated that it will be appealing against the decision.[7]

On 24 April 2024, Spotify, through X (formerly Twitter), alleged that "Apple continues to break European law". Spotify's chief public officer further stated that "By charging developers to communicate with consumers through in-app links, Apple continues to break European law. It is past time for the Commission to enforce its decision so that consumers can see real, positive benefits."[8]

Spotify claims Apple rejected their attempt to communicate with customers about their prices unless Spotify pays Apple an extra charge to communicate with consumers through in-app links.[9]

Spotify alleges that, to circumvent the DMA, Apple has purposely created an alternative to the status quo of the 30% commission fee it charges for in-app purchases, where the developers have to pay Apple a €0.50 fee for every customer download, in addition to a recurring 17% digital goods fee for every purchase made.[10]

The Commission is also now investigating Apple, Meta, and Google for non-compliance with the DMA over fees and self-preferencing.[11]

[4] ibid
[5] https://ec.europa.eu/commission/presscorner/detail/en/speech_24_1309
[6] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1689
[7] https://www.apple.com/newsroom/2024/03/the-app-store-spotify-and-europes-thriving-digital-music-market/
[8] https://www.engadget.com/spotify-tests-apples-resolve-with-new-pricing-update-in-the-eu-120004754.html
[9] ibid
[10] https://newsroom.spotify.com/2024-05-24/the-u-k-holds-firm-in-the-fight-for-fair-competition-with-the-dmcc-act-but-its-not-over-yet/
[11] https://www.engadget.com/the-eu-is-investigating-apple-meta-and-google-over-fees-and-self-preferencing-124147179.html

Competition Law in Malaysia

It is interesting to note that Section 10 of the Malaysian Competition Act 2010 (**CA**) provides for a similar prohibition to Article 102(a) of the TFEU as follows:

(1) An enterprise is prohibited from engaging, whether independently or collectively, in any conduct that amounts to an abuse of a dominant position in any market for goods or services.

(2) Without prejudice to the generality of subsection (1), an abuse of a dominant position may include:

(a) Directly or indirectly imposing unfair purchase or selling prices or other unfair trading conditions on any supplier or customer.

Although we have yet to see whether similar complaints will be lodged against Apple for its conduct in our jurisdiction.

Not The First Rodeo

This is not the first time Apple has been in hot water due to its anti-steering provisions.

Back in 2020, Apple was involved in a dispute with Epic Games, the developer of the popular video game Fortnite, which sought to challenge App Store rules requiring developers to use Apple's IAP system if purchases are offered in the app. Under this IAP system and its agreements with app developers, Apple collects payments made to developers, remits 70% to the developers, and keeps a 30% commission.

In late 2020, Apple introduced the Small Business Programme, which reduced Apple's commission to 15% for developers making less than one million dollars.[12]

Epic Games then implemented changes in its games to bypass Apple's payment system, which caused Apple to block its games in the App Store. This led Epic Games to file a suit in the United States District Court for the Northern District of California, citing a violation of California's Unfair Competition Law[13]. Its main complaint are as follows:

Apple had acted unlawfully in violation of California's Unfair Competition Law by:

(1) Restricting app distribution on iOS devices to Apple's App Store;

(2) Requiring in-app purchases on iOS devices to use Apple's in-app payment processor; and

(3) Limiting the ability of app developers to communicate the availability of alternative payment options to iOS device users.

These restrictions were imposed under the Developer Programme Licensing Agreement (**DPLA**), which developers were required to sign in order to distribute to iOS users.

Apple also filed a counterclaim alleging that Epic Games had breached the terms of the DPLA.

While the District Court's findings were in favour of Apple, it held that the third restriction, or the anti-steering prohibition, was anticompetitive

[12] United States District Court Nothern District of California | Case No. 4:20-cv-05640-YGR | *Epic Games Inc v Apple Inc, U.S. District Court, Northern District of California*, No. 20-05640

[13] https://cand.uscourts.gov/cases-e-filing/cases-of-interest/epic-games-inc-v-apple-inc/

and issued an injunction whereby Apple is permanently restrained in prohibiting developers from the following [14]:

(1) Including in their apps and their metadata buttons, external links, or other calls to action that direct customers to purchasing mechanisms in addition to In-App Purchasing; and

(2) Communicating with customers through points of contact obtained voluntarily from customers through account registration within the app.

It was held that while Apple is not considered a monopoly and did not engage in antitrust behaviour on nine of ten counts, Apple's conduct in enforcing anti-steering restrictions is anticompetitive.[15]

This decision was affirmed by the United States Court of Appeals for the Ninth Circuit when both Apple and Epic Games appealed.[16] In January 2024, the United States Supreme Court declined to hear the full appeals of both Apple and Epic Games, which means that although Apple remains primarily victorious, it must now allow developers to include notices about alternate payment systems in their apps available on the App Store.[17]

Separately, in March 2024, Epic Games filed an application to declare Apple in contempt of court for violating the injunction order against it.[18]

Apple sued by the United States Department of Justice (US DOJ) over its alleged monopoly of the market through its ecosystem.

On 21 March 2024, the US DOJ, together with 15 states and the District of Colombia, filed a complaint in the federal district court in New Jersey.[19]

Specifically, it is alleged that Apple intends to eliminate its smaller competitors by blocking the expansion of 'super-apps' that provide identical functionality across devices, such as:

(a) **Blocking Innovative Super Apps**. Apple has disrupted the growth of apps with broad functionality that would make it easier for consumers to switch between competing smartphone platforms.

(b) **Suppressing Mobile Cloud Streaming Services**. Apple has blocked the development of cloud-streaming apps and services that would allow consumers to enjoy high-quality video games and other cloud-based applications without the need for expensive smartphone hardware.

(c) **Excluding Cross-Platform Messaging Apps**. Apple has degraded the quality of cross-platform messaging apps, making them less innovative and secure, to compel its customers to continue buying iPhones.

(d) **Diminishing the Functionality of Non-Apple Smartwatches**. Apple has limited the functionality of third-party smartwatches, leading users to face substantial out-of-pocket costs if they choose not to continue buying iPhones.

(e) **Limiting Third Party Digital Wallets**. Apple has prevented third-party apps from offering tap-to-pay functionality, hindering the creation of cross-platform third-party digital wallets.[20]

---

[14] *Epic Games Inc v Apple Inc, U.S. District Court, Northern District of California*, No. 20-05640 | Permanent Injunction dated 21 September 2021 https://cand.uscourts.gov/cases-e-filing/cases-of-interest/epic-games-inc-v-apple-inc/
[15] https://cand.uscourts.gov/wp-content/uploads/cases-of-interest/epic-games-v-apple/Epic-v.-Apple-20-cv-05640-YGR-Dkt-814-Judgment.pdf & https://cand.uscourts.gov/wp-content/uploads/cases-of-interest/epic-games-v-apple/Epic-v.-Apple-20-cv-05640-YGR-Dkt-813-Injunction.pdf
[16] https://law.justia.com/cases/federal/appellate-courts/ca9/21-16506/21-16506-2023-04-24.html
[17]https://www.theverge.com/2024/1/16/24039983/supreme-court-epic-apple-antitrust-case-rejected
[18] https://www.reuters.com/legal/apple-denies-violating-us-court-order-epic-games-lawsuit-2024-04-13/
[19] https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets
[20] https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets

For example, Apple allows iPhone customers to send high-quality photos and videos seamlessly to one another, but multimedia texts to Android phones are slower and grainier. Apple has since improved the quality of the standard it uses to interact with Android phones via text messages, but it still maintains those messages in green bubbles, which may help perpetuate a class divide.[21]

Apple also allegedly stifled the use of non-Apple smartwatches by limiting how users interacted with them on the iPhone and used cloud streaming, location services, and web browsers on iPhones to snuff out smaller rivals.[22]

The antitrust lawsuit alleges that Apple has violated Section 2 of the Sherman Act.

Section 2 of the Sherman Act provides that every person who shall monopolise attempt to monopolise, or combine or conspire with any other person or persons to monopolise any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a misdemeanour.

Conclusion

Although the US DOJ suit against Apple is still in its infancy, we expect the outcome to have a significant impact on big tech companies, including Apple's operation worldwide, including in Malaysia.

It also seems that antitrust regulators in the West are very actively pursuing big tech companies. Google recently closed its argument in a battle with the US DOJ in U.S et al. v Google, where the US DOJ accused Google of illegally abusing its power as a monopoly. It allegedly orchestrated its business dealings with device makers like Apple and Samsung, and web browser companies like Mozilla, which runs Firefox.[23]

We look forward to seeing whether the directives imposed by the Commission or the United States Court would in the future promote or hinder competition between big tech companies. Some big tech companies might consider these directives restrictive, as this might hinder big companies from further improving their technologies, maximising capitalisation potential.

HOI JACK S'NG
Partner
Dispute Resolution | Regulatory and Compliance
hjs@lh-ag.com

AIDA FARALYANA BINTI AZLAN
Associate
Dispute Resolution | Regulatory and Compliance
afa@lh-ag.com

[21] https://edition.cnn.com/2024/03/21/tech/apple-sued-antitrust-doj/index.html
[22] ibid.
[23] https://apnews.com/article/google-antitrust-trial-search-engine-dominance-e7fa82026c31efe9c0a4fe95be014a74

DATA SECURITY IN FLEXIBLE WORKING ARRANGEMENTS

by Arissa Ahrom

Managing remote employees requires organisations to take a different approach to data security compared to managing employees working from centralised offices. With employees working from various locations, often outside the secure office environment, maintaining data security becomes more complex. The statutory recognition of flexible working arrangements ("**FWA**") in Malaysia provides employees with the right to apply to their employers for the variation of their hours, days, or place of work. Employers may then decide whether to approve or refuse such an application.

In making this decision, especially in relation to the variation of an employee's place of work to remote work, the crucial issue of data security should not be overlooked. This is because an employer's failure to ensure that adequate measures to safeguard personal data are implemented when allowing FWA could expose the organisation to prosecution for failing to comply with the Security Principle outlined in the Personal Data Protection Act 2010 ("**PDPA 2010**"). Such a failure amounts to an offence under the PDPA 2010, and if convicted, the organisation is liable to a fine not exceeding RM300,000.00 and / or imprisonment for a term not exceeding 2 years[1].

Cybersecurity and Data Breaches

In 2023, the Malaysia Computer Emergency Response Team ("**MyCERT**") received a total of 5,917 reports on cyber-related incidents[2]. While concerning, this may not accurately represent the true extent of cybersecurity breaches in the country, given that there are no general obligations for organisations to report any incidents of data breaches, apart from sector-specific requirements. For example, financial institutions and capital market entities are required to notify Bank Negara Malaysia[3] and the Securities Commission of Malaysia[4], respectively, of any cybersecurity incidents.

Minimum Security Measures

The Security Principle under the PDPA 2010 provides that data users are required to take practical steps to protect personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction[5]. In complying with the Security Principle, employers may refer to the Personal

[1] Section 5 (2) of the Personal Data Protection Act 2010
[2] https://mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b accessed on 23 June 2024
[3] Bank Negara Malaysia Risk Management in Technology (RMiT) Policy Document
[4] Securities Commission Malaysia's Guidelines on Management of Cyber Risk
[5] Section 9 of the Personal Data Protection Act 2010

Data Protection Standard 2015 and the General Code of Practice published by the Personal Data Protection Commissioner. These documents outline the general minimum security measures that must be taken. Some of the relevant measures that should be emphasised in an FWA include:

(a) Registering all employees involved in the processing of personal data;

(b) Terminating an employee's access rights to personal data after their resignation, termination or adjustments in accordance with changes in the organisation;

(c) Controlling and limiting employees' access to personal data systems;

(d) Providing authorised employees with user IDs and passwords to access personal data, and terminating such user IDs immediately when an employee no longer handles personal data;

(e) Ensuring that any transfer of personal data through removable media devices and cloud computing services are subject to the written consent of an authorised officer of the top management of the organisation and recording any such transfers;

(f) Safeguarding computer systems from malware threats and updating the back-up / recovery systems;

(g) Maintaining proper records of access to personal data periodically and making such records available for submission when directed by the Personal Data Protection Commissioner; and

(h) Ensuring that all employees involved in processing personal data always protect the confidentiality of the personal data.

Although the above measures apply to all data users, employers should assess the types of personal data in their possession and impose a level of security appropriate to each type of personal data.

Practical Steps for Employers

To safeguard data and ensure compliance with cybersecurity standards in FWA, employers can begin by implementing the following 3 practical measures:

1. Establish Clear Policies

   It is crucial to develop and communicate a comprehensive policy outlining not only clear rules and procedures of FWA but also setting out cybersecurity guidelines for employees working under FWA. This policy should detail expectations regarding data protection practices and adherence to the organisation's cybersecurity framework.

2. Secure Remote Devices & Control Access

   All devices provided to remote employees should be secured by installing firewalls to create a secure barrier between the business network and the internet. This measure can be strengthened by ensuring automatic updates or regularly updating the relevant software and operating systems to fix vulnerabilities and protect against cyber-attacks. Additionally, personal data stored on all devices should be encrypted to prevent unauthorised access.

   It is also good practice to deploy Virtual Private Networks ("**VPN**") to establish

secure, encrypted connections for remote access to company resources and adopt encrypted cloud storage solutions to securely store and share documents, setting clear protocols for data classification and access permissions.

3. Provide Ongoing Training

It is essential for remote employees to be equipped with the knowledge and practices needed to enhance the organisation's cybersecurity. Employers should conduct regular cybersecurity training sessions for employees, focusing on best practices, identifying cyber threats, and responding to incidents promptly. Additionally, having a dedicated support team equipped to assist FWA employees in managing cyber incidents can bolster security measures.

In today's digital age, organisations should not shy away from adopting FWA to accommodate diverse work styles and enhance productivity. By taking proactive steps to educate employees, establish clear policies, and enhance cybersecurity measures, organisations can effectively mitigate risks associated with FWA while fostering a secure and productive work environment.

ARISSA AHROM
Senior Associate
Cyber Data Privacy | Employment & Industrial Relations
aa@lh-ag.com

LAW ON REMUNERATION OF A LIQUIDATOR

by Kumar Kanagasingam, Timothy Chong Meng Soon & Michelle Louis

Like any other profession, a liquidator is entitled to receive remuneration. However, in Malaysia, there is no fixed method for determining how a liquidator should be compensated for their work in a winding up proceeding. By virtue of Section 479(2) of the Companies Act 2016 ("**CA 2016**"), a liquidator is entitled to receive remuneration by way of percentage, or otherwise as is determined by: (a) an agreement between the liquidator and the committee of inspection ("**COI**"); (b) if there is no agreement or COI, a resolution passed at a creditors' meeting by a majority of not less than three-fourths in value and one-half in number of creditors present at the meeting; or (c) if the agreement or determination under paragraph (a) or (b) fails, at the behest of the court.

At this juncture, it is imperative to highlight that a reading of the said Section 479(2) of the CA 2016 mandates that there must either be (a) an agreement with the COI as to the liquidators' remuneration, or alternatively (b) a resolution passed at a meeting of creditors in accordance with Section 479(2)(b) of the CA 2016. Failure to comply with either of the subsections will render the court being unable to hear the application due to the express words in Section 479(2)(c) of the CA 2016, specifically "*if the agreement or determination under paragraph (a) or (b) fails, the Court*". Clearly, only if either subsection (a) or (b) fails, then and only then will the court be able to determine the liquidators' remuneration (See: *Poly Ritz Development Sdn Bhd v Datuk Tee Guan Pian* [2020] 1 LNS 2279).

In this legal alert, we will examine how the court evaluates the rationale behind liquidators' remuneration when the same is challenged by a contributory under Section 479(3) of the CA 2016.

Brief Facts

The Court of Appeal's decision in *Emiprima Sdn Bhd v Wonderful Castle Sdn Bhd (in Liquidation)* [2023] 5 MLJ 695 involves an application for the review of the liquidator's remuneration. In this case, following the winding-up of Wonderful Castle Sdn Bhd ("**Respondent**"), the liquidator released the sum of approximately **RM148 million** from the sale of its assets and then called for a meeting to approve a resolution to pay him approximately **RM9 million** as his fees, computed based on Table C of the Companies (Winding-Up) Rules 1972 ("**CWUR**"). All members of the COI approved the resolution, except for Emiprima Sdn Bhd ("**Appellant**"), a contributory of the Respondent. The Appellant, dissatisfied with the COI's decision, applied to the High Court vide Section 479(3) of the CA 2016 to assess and vary the liquidator's remuneration.

<u>High Court</u>

The High Court dismissed the application,

holding that based on Table C of the CWUR, the liquidator was entitled to charge RM9 million as his fees, and that it did not offend the principle of fairness and reasonableness.

Court of Appeal

On appeal, the main question to be determined was whether the High Court was correct in accepting the determination of the remuneration solely based on the percentage listed in Table C of the CWUR without making any assessment. The Court of Appeal held that (a) Table C of the CWUR cannot be used as of right by a liquidator to calculate remuneration; and (b) the liquidator therein had failed to provide any justification for the amount claimed.

The Court of Appeal reaffirmed their decision in *Ong Kwong Yew & Ors v Ong Ching Chee & Ors and other appeals* [2018] MLJU 2189, which followed the High Court's decision in *Perumahan NCK Sdn Bhd v Mega Sakti Sdn Bhd* [2005] 7 MLJ 389, specifically in relation to the two key principles relating to the determination of the liquidators' remuneration, namely, (a) the burden of proof lies with the liquidators to show that the remuneration claimed is justifiable; and (b) the benchmark in the assessment process is fairness and reasonableness.

What Is Fair and Reasonable?

Following the recent ruling in ***Emiprima (supra)***, it is evident that in Malaysia, the pivotal benchmark for determining the quantum of a liquidator's remuneration rests upon the principles of "fairness and reasonableness". However, due to the subjective nature of these terms, clarity is crucial. We will take a closer look at the various approaches adopted by the courts across jurisdictions like Singapore, England, Australia, and Hong Kong in assessing liquidators' remuneration, with the aim of shedding light on the nuanced interpretations of "fairness and reasonableness".

Singapore

Like Malaysia, Singapore also prioritises fairness and reasonableness as the benchmark in its assessment process. This principle was articulated in the Singapore High Court decision in *Re Econ Corp Ltd (In Provisional Liquidation) (No 2)* [2004] 2 SLR 264. In this case, the Singapore High Court thoroughly examined different aspects of the liquidator's claimed remuneration and outlined several principles to guide the determination of the liquidator's remuneration. It is noteworthy that the Singapore High Court acknowledged that the list

is not exhaustive and that the guidelines are not immutable rules.

A summary of the principles are as follows:

(i) **Valued contributions**

The impact the liquidator has made on the matter.

(ii) **Amount of time spent**

The importance of this factor will vary from case to case, being crucial in one case and just another consideration in another.

(iii) **Rates**

In the absence of acceptable guidelines, rates cannot be accepted at face value. The determination of fair and reasonable rates depends on the complexity of the matter.

(iv) **Assistance rendered by the employees from the liquidator's firm**

This factor will be subject to strict proof.

(v) **Scope of work**.

(vi) **Disbursements**

There must be some measure of restraint and discipline on how the items are recouped and accounted for.

Australia

Following the decision in *Sanderson as Liquidator of Sakr Nominees Pty Ltd (in liquidation) v Sakr* [2017] NSWCA 38, the Australian Court set out the general principles and test to be adopted when assessing the remuneration to be accorded to a liquidator. Although the legislative provisions differ, the following established principles are equally applicable to the assessment of remuneration in our jurisdiction:

(i) The onus is on the liquidator to establish that the sum claimed is reasonable;

(ii) The liquidator is required to provide material on which the court can undertake a reasonable analysis; and

(iii) The court is to determine the liquidator's remuneration by evaluating the remuneration due based on the materials before it with an independent mind.

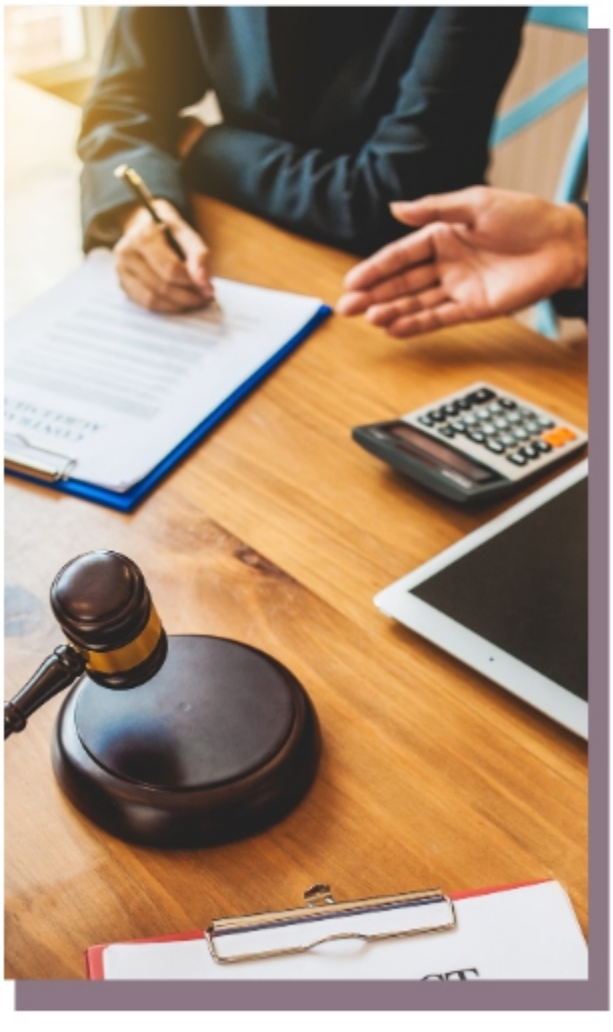
Hong Kong

The Hong Kong statutory framework is, by and large, identical to that in Singapore. The Court of Appeal in *Re Peregrine Investments Holdings Ltd* [1999] 3 HKC 291 held that:

(i) The liquidators had to provide full particulars to justify the amount of any claim for remuneration;

(ii) Where charges are sought to be recovered on a time-costs basis, the liquidators are not allowed to simply list the total number of hours spent by themselves including their staff and apply their normal charging rate. Instead, they must explain exactly what they did and why they did it; and

(iii) The liquidators must keep proper records of what they have done and why they have done it. Without contemporaneous records, they will be in a difficult position in discharging their duty to account.



Conclusion

Quite clearly, the common factor in determining liquidators' remuneration is the principle of reasonableness in the abovementioned jurisdictions. The Malaysian courts' stance on this matter mirrors that of the other jurisdictions. In Malaysia, like the abovementioned jurisdictions, liquidators are expected to justify the remuneration claimed.

It therefore appears that the percentage in Table C of the CWUR should not be taken for granted by a liquidator, as they are required to show that their remuneration is fair and reasonable. Evidently, the Court is becoming more hesitant in approving liquidators' remuneration by solely relying on Table C of the CWUR, especially when there is a lack of justification or evidence from the liquidators to support their remuneration requests.

KUMAR KANAGASINGAM
Senior Partner
Dispute Resolution
kk@lh-ag.com

TIMOTHY CHONG MENG SOON
Associate
Dispute Resolution
cms@lh-ag.com

MICHELLE LOUIS
Associate
Dispute Resolution
mil@lh-ag.com

NAVIGATING THE CIVIL FRAUD LANDSCAPE: STRATEGIES FOR ASSET TRACING & RECOVERY

by Nicola Tang Zhan Ying

"This article discusses the legal framework for combating civil fraud and tracing assets for recovery through civil proceedings in Malaysia."

Recent high-profile cases in Malaysia have highlighted the importance of civil asset recovery as a powerful tool to tackle the rising tide of fraud and financial crime.

This article will provide an overview of civil fraud and asset recovery in Malaysia, focusing on identifying, tracing and seizing, which will ultimately lead to recovery of assets acquired through fraudulent means. By enhancing awareness and understanding of the legal framework in place, stakeholders can better navigate the complexities and work toward a more robust and effective recovery regime.

1. Legal Framework – Civil Fraud

Should you or your business become a victim of fraud, the primary legal consideration is identifying the specific nature of your claim and the responsible parties. An action premised on civil fraud enables a defrauded plaintiff to recover losses and damages caused by fraudulent behaviour.

"*Civil fraud*" does not constitute a legal action in itself; it is an umbrella term encompassing various heads of legal claims. The plaintiff bears the burden of proving such claims on the balance of probabilities. This burden of proof is lower than the that required in criminal proceedings, which is beyond a reasonable doubt. Outlined below are the most common types of causes of actions for civil fraud claims and the available remedies.

Fraudulent Misrepresentation / Tort of Deceit

Fraudulent misrepresentation falls under the tort of deceit. To succeed in a claim for fraudulent misrepresentation, the plaintiff must establish[1]:

(a) The defendant made a false statement or representation.

(b) The defendant knew the statement or representation was false or was reckless as to whether it was false;

(c) The defendant intended for the plaintiff to rely on that statement;

(d) The plaintiff relied on the false statement; and

(e) The plaintiff suffered loss as a result.

[1] *Victor Cham & Anor v Loh Bee Tuan* [2006] 5 MLJ 359, Court of Appeal (CA) at para [13]. As for the elements of the tort of deceit see *Panatron Pte Ltd and another v Lee Cheow Lee and another* [2001] SGCA 49, Court of Appeal of Singapore at paras [14] and [23]

Rescission is often the primary remedy pursued because fraudulent misrepresentation renders the contract voidable. The contract will be set aside, and the parties are put back in their original positions before the contract was made. However, the victim of fraud may elect to abandon their right to rescind and instead insist on the performance of the contract, placing them in the position they would have been if the representations made were true[2].

The plaintiff is also entitled to claim tortious damages to compensate for the loss incurred. The objective of the law is to put the victim in the position they would have been in if the tort had not been committed. Hence, the rule as to the remoteness of damage contained in Section 74 of the Contracts Act 1950 does not apply[3]. The plaintiff can recover damages for all losses suffered directly due to their reliance on the false statement, even if the loss was not reasonably foreseeable. Of note, when the conduct of the wrongdoer discloses fraud, exemplary damages may be ordered[4].

Unlawful Means Conspiracy

This is an economic tort. The plaintiff must establish[5]:

(a) There was an agreement between two or more people to act together unlawfully, with the intention of causing harm to the plaintiff; and

(b) The concerted action caused damage to the plaintiff.

The agreement to conspire does not necessarily refer to a written agreement or a formal arrangement[6]. The intention to cause damage need not be the predominant purpose; an intention to inflict harm suffices.

A company, as a separate legal entity, can conspire with its directors. The knowledge of the company may be imputed from the person who has management control (typically a director acting as its alter ego) for the transaction or act in question[7]. Conspirators who use unlawful practices are liable for any damage that results from their unlawful concerted practices.

Dishonest Assistance

As a general rule, there must be a breach of trust or fiduciary duty by someone other than the defendant, and the defendant must have helped that person in the breach. It is the person assisting who must be shown to have had a dishonest state of mind[8]. Without a finding of dishonesty on the part of the person assisting, the finding of 'knowing assistance' is not sufficient[9]. In a breach of trust situation, subjective dishonesty is relevant[10].

The elements that must be proved to establish dishonest assistance are[11]:

(a) There has been a disposal of assets in breach of trust or fiduciary duty;

(b) The defendant has assisted or procured the breach;

(c) The defendant acted dishonestly; and

(d) There is resulting loss to the plaintiff.

[2] Contracts Act 1950, s 19(2)
[3] *Abdul Razak Bin Datuk Abu Samah v Shah Alam Properties Sdn Bhd and Another Appeal* [1999] 2 MLJ 500, CA at 508-509
[4] *Lembaga Kemajuan Tanah Persekutuan (FELDA) & Anor v Awang Soh bin Mamat & Ors* [2009] 4 MLJ 610, CA at para [144].
[5] *Renault SA v Inokom Corp Sdn Bhd & Anor and other appeals* [2010] 5 MLJ 394, CA at p 406
[6] Ibid, p 406
[7] *Tekital Sdn Bhd v Sarina bt Kamaludin & Ors* [2012] 8 MLJ 734, at paras [93]-[96]
[8] *Kuan Pek Seng @ Alan Kuan v Robert Doran & Ors and other appeals* [2013] 2 MLJ 172, CA at para [55]-[56]
[9] Ibid para [65]. See also *Barnes v Addy* (1874) LR 9 Ch App 244
[10] *CIMB Bank Bhd v Maybank Trustees Bhd and other appeals* [2014] 3 MLJ 169, Federal Court ("FC") at para [146]; citing *Twinsectra Ltd v Yardley* [2002] UKHL 12
[11] *Jaya Sudhir a/l Jayaram v Dato' Seri Timor Shah Rafiq & Ors and another case* [2020] 1 LNS 1975 at para [337], which cited Caltong (Australia) Pty Ltd (formerly known as *Tong Tien See Holding (Australia) Pty Ltd) and another v Tiong Tien See Construction Pte Ltd (in liquidation) and another appeal* [2002] 3 SLR 241 (SGCA) at para [33]. See also *Royal Brunei Airlines Sdn Bhd v Philip Tan Kok Ming* [1995] 2 AC 378; [1995] 3 All ER 97

An accessory is liable for the loss occasioned by their dishonest assistance to the same extent as the principal, but only with respect to the breach they knowingly assisted. For accessory liability, the accessory must know they are dealing with someone in a fiduciary relationship and owed a duty to act in good faith[12]. The plaintiff may be awarded equitable compensation, a discretionary monetary remedy. Alternatively, the courts also have the discretion to order the defendant to account for any gain or profit obtained through dishonest assistance, irrespective of whether the wrongdoing caused any corresponding loss to the plaintiff.

Knowing Receipt

Central to the concept of knowing receipt is the proof of dishonesty on the part of the recipient[13]. The elements of knowing receipt are as follows[14]:

(a) Disposal of assets in breach of fiduciary duty;

(b) The beneficial receipt by the defendant of assets which are traceable as representing the assets of the plaintiff; and

(c) Knowledge on the part of the defendant that the assets received are traceable to a breach of fiduciary duty.

If a property is transferred in breach of trust to a third party who is not a bona fide purchaser for value without notice (i.e., an innocent party unaware of any existing claims to the property's title), the plaintiff will have a claim to that property[15]. The plaintiff may also pursue equitable compensation or an order for the account of profits as a remedy.

Unjust Enrichment

A cause of action in unjust enrichment can give rise to a right to restitution where it can be established that[16]:

(a) The defendant has been enriched;

(b) The enrichment was gained at the plaintiff's expense;

(c) The defendant's retention of the benefit is unjust; and

(d) There is no defence available to extinguish or reduce the defendant's liability to make restitution to the plaintiff.

The law of unjust enrichment can apply to the rights of parties to a contract that has been validly terminated. The usual remedy is that the plaintiff is entitled to restitution, whereby the defendant must pay the value of the enrichment.

[12] *Menno Leendert Vos v Global Fair Industrial Limited & ors* [2009] HKCU 1910
[13] *Ooi Meng Khin v Amanah Scotts Properties (KL) Sdn Bhd* [2014] 6 MLJ 488, CA at para 34
[14] *LNE Network Systems (Asia) Sdn Bhd v Loi Chew Ping & Ors* [2015] 3 CLJ 663, citing *El Ajou v Dollar Land Holdings plc and another* [1994] 2 All ER 685
[15] *Ikumi Terada v Jemix Co. Ltd & Ors and other appeal* [2019] MLJU 561; applying *Foskett v McKeown* [2000] 3 All ER 97
[16] *Dream Property Sdn Bhd v Atlas Housing Sdn Bhd* [2015] 2 CLJ 453, FC at paras [110], [117] and [118]

Tort of Conversion

This is the civil version of theft. Conversion occurs when someone without the right to deal with your property deprives you of its use and enjoyment.

A plaintiff must prove[17]:

(a) The defendant's conduct was inconsistent with the rights of the owner;

(b) The defendant's conduct was deliberate, not accidental; and

(c) The defendant's conduct encroached on the rights of the owner, excluding the owner's use and possession of their personal property.

If it is demonstrated that the defendant intended to seize or interfere with the property, there is no need to prove that the defendant intended to commit a wrong. A claim for conversion can arise in various circumstances, but it often involves misappropriation, which frequently includes fraud.

Damages in conversion cases aim to compensate and restore the affected party to their original position. The remedy includes the return of the goods or damages equivalent to the market value[18] of the goods lost.

2. Immediate Actions: Securing Assets and Pursuing Recovery

To safeguard their position and enhance chances of recovery, victims of fraud and financial scams must act swiftly. The following immediate steps are vital:

(a) *Preventive measures to preserve assets and minimise further potential losses:*

- Preserve financial, IT, and communication data and records: Ensure all relevant data is securely stored, backed up, and readily accessible for review.
- Conduct internal investigations: Identify and pinpoint personnel involved in questionable transactions.
- Notify banks and financial institutions: Instruct them to freeze relevant accounts pending civil and/or criminal proceedings. Banks are required to promptly investigate notices of fraudulent transactions and take protective measures, even if it originates from parties with whom they have no direct relationship[19].

(b) *Legal Action and Interim Reliefs*

- Develop a legal strategy for recovery.
- Determine the cause of action.
- Identify which party to sue.
- Assess the need for interim reliefs such as Norwich Pharmacal Orders, Anton Pillar Orders, and Mareva Injunctions.

(c) *Obtain Evidence and Conduct Fact-Finding*

Consider the available evidence and whether it is sufficient. This may involve working with forensic IT experts, accountants, private investigators, and solicitors. It is advisable to involve solicitors at this fact-finding stage to ensure the findings are protected by privilege.

---

[17] *Zung Zang Wood Products Sdn Bhd & Ors v Kwan Chee Hang Sdn Bhd & Ors* [2014] 2 CLJ 445; see also *Tay Kian Hock v Kewangan Bersatu Bhd* [2002] 4 MLJ 411

[18] *KFH Siarah House (M) Sdn Bhd v Lembaga Kemajuan Wilayah Pulau Pinang* [2013] 3 MLJ 850

[19] *Nemonia Investments Ltd v AmBank Islamic Berhad & 3 Ors* [2023] 8 AMR 201

3. Asset Tracing & Recovery Strategies

Proactive and speedy measures such as collation of evidence, asset tracing, and securing freezing orders or injunctions are vital to preserve assets pending litigation. Criminal asset forfeiture hinges on a conviction. On the other hand, civil asset recovery proceedings target the property itself, not the individual. This means the standard of proof in civil asset recovery is lower; i.e., on a balance of probabilities rather than beyond a reasonable doubt.

The civil remedies under the Malaysian Court system provide various interim reliefs to ringfence assets pending disposal of the action and to obtain evidence in the event of suspected fraud.

A. Preservation of Assets[20]

Mareva Injunction[21]

This is a court order freezing the defendant's assets up to a certain value, preventing the dissipation of assets within or outside the jurisdiction pending full and final disposal of the matter. The applicant may also seek the discovery of information or documents to support the Mareva Injunction and determine the location of assets.

To obtain a Mareva Injunction, the applicant must demonstrate:

(a) A good arguable case against the defendant;

(b) A real risk of the defendant dissipating assets; and

(c) It is just and convenient to grant the injunction.

A risk of dissipation can be inferred if the defendant acted dishonestly in bad faith, maintains foreign accounts, and there is evidence of fund transfers to these accounts[22].

Such an application can be made ex-parte but is valid for only 21 days from the date of the order. The plaintiff is required to make full and frank disclosure of all relevant facts, especially those unfavourable to their case. Failure to do so can result in the ex-parte order being set aside. Furthermore, the applicant must provide an undertaking to the court to compensate the defendant for any damages if it is later determined that the injunction was incorrectly granted. The applicant may also need to furnish security for this undertaking. An inter partes hearing will be fixed within 14 days of the ex-parte order being granted. Once served with the

---

[20] Injunctions are governed by Order 29 Rule 1 of the Rules of Court 2012.
[21] *Mareva Compania Naviera SA v International Bulkcarriers SA* [1980] 1 All ER 213
[22] *Securities Commission v Lee Kee Sien, Albert & Ors* [2009] 8 CLJ 70, HC. See also *Jasa Keramat Sdn Bhd v. Monatech (Malaysia) Sdn Bhd* [1999] 4 CLJ 430 at p 38 h-i where the Court held probity and conduct of the defendant is relevant to risk of dissipation of assets.

court order, third parties, including banks, are obliged to comply or they run the risk of being held in contempt of court[23].

The purpose of a Mareva Injunction is to prevent an abuse of the legal process, where a party facing judgment intentionally dissipates assets to avoid satisfying it. Therefore, the courts have recently held that factors such as where the balance of convenience lies, the adequacy of damages, and the potential irreparable harm caused by not granting the interlocutory injunction should not be considered in a Mareva application[24].

Proprietary Injunction

A proprietary injunction is a remedy that latches on to an asset over which the plaintiff asserts a proprietary interest. The asset sought to be preserved includes those that are monetary in nature[25]. Unlike a Mareva Injunction, it does not require proof of the risk of dissipation[26]. An applicant can pursue both a Mareva Injunction and a Proprietary Injunction concurrently.

The applicant must establish[27]:

(a) There is a bona fide serious question to be tried;[28]

(b) The balance of convenience lies in granting the injunction; and

(c) Damages would not be an adequate remedy.

B. Obtaining Evidence

*Pre-action Discovery under the Rules of Court 2012 ("**RC 2012**")*

Order 24 Rule 7A, RC 2012 permits pre-action discovery applications against potential wrongdoers or defendants. In pre-action discovery, the applicant seeks to determine whether they have a viable claim against the intended defendant

The applicant must demonstrate:

(a) Pre-action discovery, and not discovery in the course of action or proceedings, is necessary;

(b) The respondent to the application has in its possession, custody, or power the documents sought to be discovered;

(c) The documents sought are relevant to an issue arising or likely to arise in the intended proceedings;

(d) The documents sought are necessary to determine whether there is a viable cause of action for the plaintiff (which is the main question determining whether discovery will be granted); and

---

[23] *Monatech (M) Sdn Bhd v Jasa Keramat Sdn Bhd* [2002] 4 CLJ 40

[24] All Kurma Sdn Bhd v Teoh Heng Tatt & Ors [2023] 7 MLJ 303, at para [102]; citing Lee Kai Wuen & Anor v Lee Yee Wuen [2022] 1 LNS 1057, CA at paras [112]-[122]

[25] *Pacific Rainbow International Inc v Shenzhen Wolverine Tech Ltd and Others* [2017] HKCU 1076

[26] *Zschimmer & Schwarz GmbH & Co KG Chemische Fabriken v Persons Unknown & Anor* [2021] 7 MLJ 178

[27] *Keet Gerald Francix Noel John v Mohd Noor Bin Abdullah* [1995] 1 MLJ 195, p 206-207; adopting the test of *American Cynamid v Ethicon Limited* [1975] AC 396

[28] This is typically achieved by demonstrating an arguable case in support of the applicant's claim of a proprietary interest in the assets.

(e) The discovery is necessary either for disposing fairly of the cause or matter or for saving costs.

When deciding whether to grant pre-action disclosure, the court must balance the competing interests of various parties, including third parties. Given the importance of personal and commercial confidentiality, safeguards and limited or redacted disclosures may be imposed. The application will be refused if the applicant already knows their cause of action and is not otherwise prevented from commencing proceedings against the intended defendant.

*Norwich Pharmacal Order ("**NPO**")*[29]

This common law pre-action discovery order is used to obtain information from a third party or non-party to reveal the identity of potential wrongdoers, before commencement of an action. The legal concept behind an NPO is that if an innocent person becomes unintentionally involved in the wrongful acts of others, they have a duty to assist the injured party by providing complete information and disclosing the identities of the wrongdoer.

An NPO is discretionary and not automatically granted. The order will only be issued if the applicant demonstrates that the interest of justice in allowing the discovery outweighs the public interest in maintaining confidentiality.

To succeed in such an application, the applicant must demonstrate:

(a) The third party/non-party facilitated the wrongdoing, whether innocently or otherwise;

(b) There is a good arguable case against the potential wrongdoer(s) whose identity is being sought; and

(c) Disclosure is necessary to enable him to take action, or at least that it is just and convenient in the interest of justice to make the order sought.

An NPO may be accompanied by a gagging order to prevent alerting the wrongdoers or fraudsters about the ongoing investigation and tracing efforts.

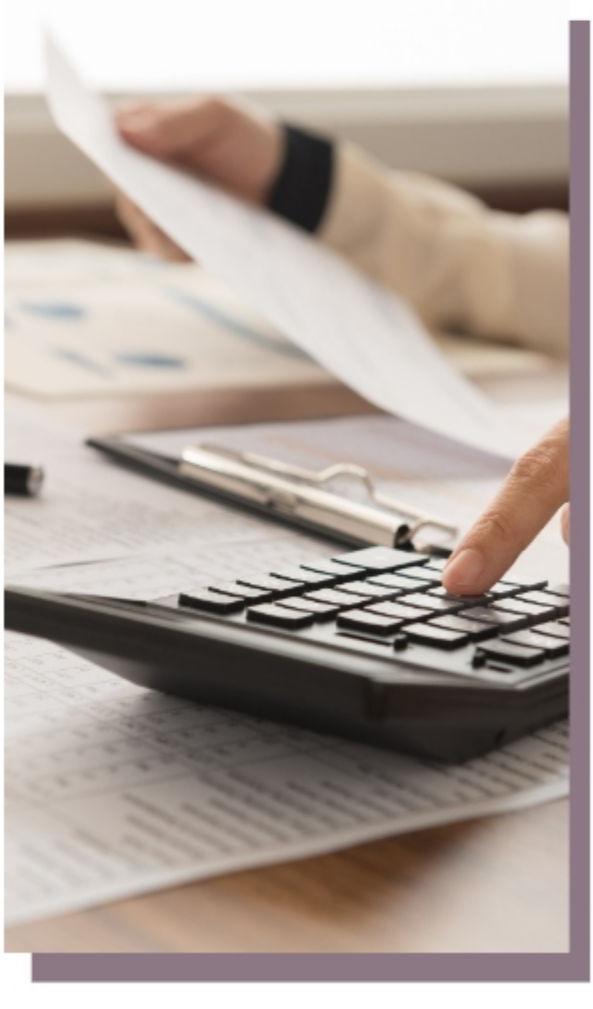
*Bankers Trust Order ("**BTO**")*[30]

A BTO, a variation of an NPO, compels a third party or non-party to fully disclose information to determine the whereabouts of the plaintiff's assets, funds, or monies. Typically issued against a bank, a BTO serves as an exception to banking secrecy.

Similar to an NPO, the grant of a BTO is not as of right and is a matter of discretion. In addition to meeting all the criteria for a Norwich Pharmacal Order, the applicant must demonstrate a strong reason to believe that the bank holds property misappropriated by fraud or breach of trust, to which the applicant has a proprietary claim. It must also be demonstrated that the information will be used exclusively for tracing funds.

Anton Pillar Order[31]

An Anton Piller Order, often referred to as a civil search warrant, is generally granted ex-parte. It permits the applicant to enter and search the premises to enable an inspection, seizure, and removal of relevant documents and property. It is often used in conjunction with a Mareva Injunction in fraud or breach of trust cases, particularly where dishonest wrongdoers are likely to destroy evidence.



[29] *Norwich Pharmacal Co. & Others v Customs & Excise Commissioners* [1974] A.C 133
[30] *Bankers Trust Co v Shapira and Others* [1980] 1 WLR 1274 at p 1275; applied in *Tey Por Yee & Anor v Protasco Bhd & Ors* [2020] 5 CLJ 216 at p 251
[31] *Anton Piller KG v Manufacturing Processes Ltd and Others* [1976] 1 All ER

The applicant must fulfil the following elements:

(a) Demonstrate an exceptionally strong prima facie case;

(b) Provide clear evidence that the defendant possesses incriminating materials at risk of being destroyed; and

(c) Show that the damage to the applicant, potential or actual, is very significant without the order.

Given the draconian nature of this remedy, the applicant bears the burden of making full and frank disclosure. Failure to do so is likely to result in the setting aside of the ex-parte order and a claim for damages by the defendant.

4. Concluding Remarks

Malaysia is rapidly advancing as a financial hub. Recent legislative updates underscore its proactive stance in adapting to current financial demands, while the country benefits from various international investments.

On the regulatory front, bodies such as the Securities Commission Malaysia (SC), Bank Negara Malaysia (BNM), and the Malaysian Anti-Corruption Commission (MACC) play pivotal roles in detecting and prosecuting civil fraud. The MACC, empowered by the Anti-Money Laundering and Anti-Terrorism Financing Act 2001 (AMLATFPUAA 2001), is particularly instrumental in enforcing the recovery of stolen assets. This can be seen from the Malaysian Anti-Corruption Commission's (MACC) pledge to improve governance and institutionalise integrity to revive the country's economy through asset recovery operations. The synergy between regulatory authorities and private practitioners, coupled with a blend of parallel civil and criminal litigation, has proven to be a formidable approach in the ongoing battle against fraud and for the recovery of assets.

With a strong legal framework rooted in common law, Malaysia is well-equipped to tackle civil fraud by drawing upon English legal principles, equity doctrines, as well as precedents from other common law jurisdictions. This bolsters our position as a leading financial center and strengthens our capacity to protect financial integrity amidst global challenges.

NICOLA TANG ZHAN YING
Partner
Asset Recovery | Corporate & Commercial Disputes
tzy@lh-ag.com

LH AG ADVOCATES AND SOLICITORS

WE'RE HERE TO HELP!

Get in touch with us:
Phone: +603 6208 5888
Fax: +603 6201 0122
Email: enquiry@lh-ag.com

Visit us at:
Level 6, Menara 1 Dutamas,
Solaris Dutamas,
No. 1, Jalan Dutamas 1,
50480, Kuala Lumpur, Malaysia

For additional information regarding the Legal Herald, kindly contact updates@lh-ag.com or your designated representative.

We appreciate and welcome your opinions, comments, and suggestions.

About Lee Hishammuddin Allen & Gledhill

The firm has over 90 lawyers in Kuala Lumpur, Penang, and Johor Bahru. Our areas of practice include the following specialised practice groups, each led by an experienced partner:

Adjudication
Arbitration
Banking & Insolvency
Capital Markets
Construction
Corporate & Commercial Disputes
Employment & Industrial Relations
Financial Services
FinTech
Foreign Investment
Insurance
IP & TMT
Islamic Finance
Mergers & Acquisitions
Oil & Gas
Planning & Environment
Projects & Construction
Real Estate
Regulatory & Compliance
Securities Litigation
Shipping
Tax, Customs & Trade
Trust, Probate & Administration
White Collar Crime

Published by

Lee Hishammuddin Allen & Gledhill