Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top-ranked lawyers

International Fraud & Asset Tracing

Singapore
Danny Ong, Jansen Chow and Yam Wern-Jhien
Rajah & Tann Singapore LLP

practiceguides.chambers.com

2021

SINGAPORE

Law and Practice

Contributed by:
Danny Ong, Jansen Chow and Yam Wern-Jhien
Rajah & Tann Singapore LLP see p.12

CONTENTS

1. FRAUD CLAIMS

1.1 General Characteristics of Fraud Claims

As a trading and financial hub, there is often an international element to fraud claims in Singapore. The general characteristics of fraud claims in Singapore include:

- the making of false statements;
- misappropriation or diversion of assets (particularly through multiple and offshore entities);
- falsification of documents and banking records;
- conspiracy to defraud (including between individuals and the corporate entities used to perpetrate the fraud);
- breach of fiduciary duties by an agent or officer of a company;
- dishonest assistance; and
- corrupt payments.

1.2 Causes of Action after Receipt of a Bribe

The principal's cause of action may be founded on restitution (money had and received) or breach of fiduciary duty (prohibition against secret profits). The latter is relevant if the principal also intends to seek a constructive trust over the bribe and trace the proceeds thereof.

A principal's right at law to recover the bribe or the monetary value of the bribe received by its agent is statutorily recognised. Section 14 of the Prevention of Corruption Act provides that a principal may recover as a civil debt the amount or monetary value of the bribe received by the agent, or from the person who gave the bribe, and no conviction or acquittal of the defendant shall operate as a bar to recovery. The fact that the agent had paid fines equivalent to or in excess of the value of the bribe received is not a bar to recovery by the principal. The possibility of double disgorgement acts as a further deterrent against corruption.

1.3 Claims against Parties Who Assist or Facilitate Fraudulent Acts

The party who assisted or facilitated the fraudulent acts of another may be liable in a claim for:

- unlawful means conspiracy, together with the primary wrongdoer, if the fraudulent acts were carried out by one or more of them pursuant to conspiracy between them to injure the victim;
- dishonest assistance, if that party assisted or facilitated the breach of fiduciary duties; or
- knowing receipt, where the assistance/facilitation involved the receipt of trust/proprietary funds.

1.4 Limitation Periods

Generally, causes of action grounded in contract and tort are subject to a six-year limitation period (see Section 6 of the Limitation Act).

There are, however, specific provisions that deal with claims based on fraud. For instance:

- under Section 22 of the Limitation Act, no period of limitation shall apply to an action by a beneficiary under a trust, being an action in respect of any fraud or fraudulent breach of trust to which the trustee was a party or privy, or to recover from the trustee trust property or the proceeds thereof in the possession of the trustee or previously received by the trustee and converted to his use; and
- under Section 29 of the Limitation Act, the six-year limitation period shall not begin to run in certain cases of fraud or mistake until the plaintiff has discovered the fraud or mistake, as the case may be, or could with reasonable diligence have discovered it.

1.5 Proprietary Claims against Property

Generally, a victim of a fraud may make a proprietary claim for the misappropriated funds or property, and seek a constructive trust to be imposed over the funds or property. The constructive trust will give priority to the claimant against other unsecured creditors in an insolvency situation. It also enables the claimant to trace and follow the fraud proceeds. Hence, if the proceeds of fraud are invested successfully before they are recovered by the victim, the victim is entitled to trace the fraud proceeds into the investment and claim the full value of thereof.

Where the proceeds of the fraud have been commingled, there are specific rules and methods of distribution that the Singapore court may apply in considering the distribution of such commingled funds, depending on whether the assets were commingled with the assets of the fraudster, or that of other innocent third parties, and whether and how the commingled funds have been spent or dissipated. In the case of the former, the courts will apply the rule that is most favourable to the victim. The courts may apply the presumption (which is rebuttable) that the fraudster had spent his own money first and the remaining money is the beneficiary's (if the victim seeks to claim the remaining funds), or the presumption that the beneficiary's money was spent first (if the victim seeks to trace the proceeds of the funds). In the case of the latter, the courts may order a pro rata distribution from the commingled assets.

1.6 Rules of Pre-action Conduct

There are no rules of pre-action conduct required of a claimant in relation to fraud claims. There is generally no obligation to provide any advance notice or to undertake any alternative dispute resolution prior to the commencement of any legal proceedings (unless otherwise agreed between the parties).

1.7 Prevention of Defendants Dissipating or Secreting Assets

A claimant may seek either a freezing injunction (in personam) over the defendant to prevent him or her from dealing with or disposing of assets beyond a certain value, or a proprietary injunction (in rem) over a specific asset in which the plaintiff asserts a proprietary interest. Such injunctions are typically sought on an urgent and without notice (ex parte) basis. Freezing injunctions can be sought either in aid of domestic or foreign proceedings, although the legal requirements for each differ.

A claimant may also seek a freezing injunction against a third party (non-cause of action defendant) who is holding onto the defendant's assets as nominee.

Exceptionally, a claimant may also seek an interim receivership order requiring the defendant's assets to be handed over and managed by a court-appointed receiver, pending trial of the action. A receivership order may be granted if the court concludes that the defendant cannot be trusted to obey the freezing order, for example, where the defendant's assets are held via a complex, opaque and multi-layered corporate structure.

If the defendant does not comply with the court order, he may be liable for contempt of court under the Administration of Justice (Protection) Act for a fine up to SGD100,000, or imprisonment for a term not exceeding three years, or both. Additionally, the court may refuse to hear the defendant until the contempt is purged, or the defendant submits to the order or direction of the court, or an apology is made to the satisfaction of the court. Third parties (such as banks) within Singapore are also bound by the freezing order when they receive notice of the injunction, failing which the third party may also be liable for contempt of court.

A claimant seeking a freezing or proprietary injunction will need to pay filing fees for the application, which may range between SGD2,000 to SGD10,000, depending on the volume and number of documents filed. The fees are not pegged to the value of the claim. The claimant will also be required to provide a cross-undertaking in damages to the court, which may be substantial depending on the nature of the claim and the potential loss and damage that may be incurred by the defendant. In certain cases, the claimant may also be required to provide fortification of such undertaking, which would usually be in the form of payment into court, a solicitor's undertaking, or bank guarantee.

2. PROCEDURES AND TRIALS

2.1 Disclosure of Defendants' Assets

Generally, a claimant can seek disclosure orders as an ancillary order to support the freezing injunction. The defendant will be required to file an affidavit to identify his or her assets, whether held in his or her own name or not, and whether solely or jointly owned.

If there is reasonable ground to believe that the defendant has not complied with his disclosure obligations, the claimant may apply for the defendant to be cross-examined on his or her asset disclosure. Where the defendant is found to have acted in breach of the disclosure orders, he or she may be liable for contempt of court.

A claimant may also rely on the defendant's failure to comply with the disclosure order as a basis to apply for an interim receivership order requiring the defendant's assets to be handed over and managed by a court-appointed receiver, pending trial of the action.

In any event, the claimant will be required to provide a cross-undertaking in damages to the court. In certain cases, the claimant may also be required to provide fortification of such undertaking.

2.2 Preserving Evidence

The court may grant a search order (formerly known as an Anton Piller order) to prevent a defendant from destroying incriminating evidence. Such an order permits certain persons to enter the defendant's premises to search for, seize and retain documents or other items.

Such an application is usually made on an ex parte basis. The requirements that must be satisfied in order to obtain a search order are:

- the applicant has an extremely strong prima facie case;
- the potential damage suffered by the applicant would have been very serious;
- there was a real possibility that the defendant would destroy relevant documents before an inter partes application (ie, with notice to the other party) can be made; and
- the effect of the search order would not be out of proportion to the legitimate object of the order.

Similar to an application for a freezing order, the applicant will have to undertake to pay damages that may be sustained by the defendant as a result of the search order if it is granted by the court.

2.3 Obtaining Disclosure of Documents and Evidence from Third Parties

A court application is permitted to seek disclosure of documents and evidence from third parties, either before the commencement (pre-action) or during the course of proceedings.

In either case, the applicant will be required to specify or describe the documents sought, and show how such documents are relevant to an issue arising or likely to arise out of the claim made or likely to be made, and that the documents are likely to be in the possession, custody or power of the third party against whom disclosure is sought.

In the cases of fraud and asset tracing, the courts would usually be prepared to grant pre-action disclosure orders in line with the principles for the grant of a Norwich Pharmacal order or Banker's Trust order, ie, to enable the identification of the wrongdoer or the tracing of misappropriated funds or property.

A party who is given discovery of documents pursuant to an order of court gives an implied undertaking to the court only to use those documents for the conduct of the case in which the discovery is given, and not for any collateral or ulterior purpose (also known as the "Riddick Undertaking").

As discovery on compulsion of court order is an intrusion of privacy, the Riddick principle ensures that this compulsion is not pressed further than the course of justice requires. This implied undertaking is sometimes fortified by an express undertaking to the same effect.

A breach of the undertaking amounts to a contempt of court. The Riddick principle is, however, not an absolute one, and a court has discretion to release or modify the undertaking.

2.4 Procedural Orders

Generally, an application for a freezing injunction or a search order will be made on an ex parte basis. The courts' practice directions, however, require that except in cases of extreme urgency or with leave of court, the applicant shall still be required to provide a minimum of two hours' notice to the other party before the ex parte hearing.

The applicant of an ex parte application must make full and frank disclosure to the court of all facts which are material to the exercise of the court's discretion whether to grant the relief. In other words, the applicant must disclose all matters within his knowledge which might be material, even if they are prejudicial to the applicant's claim.

2.5 Criminal Redress

Generally, the victims of fraud would seek redress concurrently through criminal and civil proceedings. The criminal prosecution and civil proceedings may progress in parallel. In less serious fraud cases, however, criminal prosecution may take place only after the conclusion of the civil claim.

As mentioned at **1.2 Causes of Action after Receipt of a Bribe**, Singapore has various statutory provisions that would capture different fraudulent acts.

For example, the Penal Code it provides for:

- dishonest misappropriation of property (Section 403);
- criminal breach of trust (Section 405);
- dishonest receipt of stolen property (Section 411);
- cheating (Section 415);
- dishonest or fraudulent disposition of property (Section 421);
- forgery (Section 463); and
- falsification of accounts (Section 477A).

The Companies Act also sets out the following conduct which, if a person is found guilty of, may amount to an offence:

- false and misleading statement (Section 401);

- false statements or reports (Section 402);
- fraud by officers (Section 406); and
- breach of directors' duty (Section 157).

2.6 Judgment without Trial

A default judgment may be obtained where a defendant fails to enter an appearance or file a defence within the stipulated timelines.

In cases where it is clear that the defence is wholly unmeritorious, the plaintiff may seek summary judgment without trial. Generally, summary judgment would be argued on affidavit evidence, and would be granted where there are no triable issues.

2.7 Rules for Pleading Fraud

The Legal Profession (Professional Conduct) Rules provide that a legal practitioner must not draft any originating process, pleadings, affidavit, witness statement or notice or grounds of appeal containing any allegations of fraud unless the legal practitioner has clear instructions to make such an allegation and has before the legal practitioner reasonably credible material which establishes a prima facie case of fraud.

In terms of the standard of proof for a fraud claim, the burden remains the same as in other civil cases – that is the civil standard, ie, on the balance of probabilities. However, the Singapore courts have observed that the more serious the allegation (which is the case in a fraud claim), the stronger or more cogent the evidence is required for the claimant to discharge his or her burden.

2.8 Claims against "Unknown" Fraudsters

There are no reported cases where the Singapore courts have granted relief against "persons unknown" in the context of fraud claims. However, it is considered that the Singapore courts have the power to grant relief in respect of proceeds of fraud or assets derived from a fraud perpetrated, even if the fraudsters are not identifiable, and will in the appropriated circumstances, exercise that power to aid the victims.

2.9 Compelling Witnesses to Give Evidence

A party can apply to the court to issue a subpoena compelling a witness to testify or produce documents.

In determining whether to grant a subpoena, the court considers whether the witnesses to be subpoenaed are in a position to give oral and/or documentary evidence relevant to the issues raised in the case.

A subpoena should not be used to fish for evidence, or to embarrass or inconvenience the person subpoenaed.

Such an application is governed by the Rules of Court. A subpoena must be served personally and within the specific timeframe stipulated in the Rules of Court.

If a witness disobeys a subpoena, the court has jurisdiction to enforce the order by committal.

3. CORPORATE ENTITIES, ULTIMATE BENEFICIAL OWNERS AND SHAREHOLDERS

3.1 Imposing Liability for Fraud on to a Corporate Entity

A company can be made liable for the acts of its directors and officers through the doctrine of attribution. Under this doctrine, the company and its officers are still treated as distinct legal entities, but the acts and the states of mind of the officers are treated as those of the company.

There are three types of rules of attribution.

First, there are primary rules of attribution that are found in the company's constitution or implied by company law, which deem certain acts by certain natural persons to be the acts of the company. For instance, if the board of directors of a company is aware of acts being performed by employees or agents of the company, knowledge of such acts could be attributed to the company.

Second, there are general rules of attribution by which a natural person may have the acts of another attributed to him or her, ie, the principles of agency, and by which a natural person may be held liable for the acts of another, such as the principles of estoppel, ostensible authority and vicarious liability.

Third, there are special rules of attribution where, although the primary and general rules of attribution are not applicable, the courts find that a substantive rule of law is applicable to the company. This would depend on the interpretation or construction of the relevant rule which the person's act or state of mind was, for the purpose of the rule, to be attributed to the company.

In particular, the special rules of attribution operate differently depending on the factual matrix. In the case of fraud, the courts have held that while a company could be bound by the improper acts of the directors at the suit of an innocent third party, that rule of attribution should not apply where the company itself is bringing a claim against the directors for their breach of duties.

3.2 Claims against Ultimate Beneficial Owners

In certain exceptional circumstances, courts can ignore the separate legal personality of a company and look to those who stand behind the companies eg, shareholders. This is typically referred to as "lifting the corporate veil".

One scenario where corporate veil can be lifted is where the company is used as by the person as an instrument of fraud. A fraudster will not be allowed to commit a wrong through a company that he or she controls and then asserts that it is the company and not himself or herself who should bear the responsibility for the wrong.

The corporate veil can also be lifted where the company is simply an alter ego of the fraudster, ie, where there is no distinction between the company and the fraudster, and the company is simply carrying on the business of its controller.

3.3 Shareholders' Claims against Fraudulent Directors

The general rule is that the proper plaintiff to bring a claim against fraudulent directors is the company itself. Shareholders are typically not allowed to sue on the company's behalf but can request the company's board of directors to take action. The shareholders of the company may also attempt to oust the fraudulent directors by way of a shareholder resolution, and then have the company bring claims against its fraudulent ex-directors.

However, in the situation where the wrongdoers are themselves in control of the company and do not allow for an action to be brought in the company's name, the minority shareholders may consider seeking leave from the court to pursue a derivative action, either under common law or statute.

Specifically, under Section 216A of the Companies Act, the shareholder may apply to court for leave to bring an action in the company's name. The court would need to be satisfied that:

- the complainant is acting in good faith; and
- it is prima facie in the interests of the company that the action should be brought.

Under the common law derivative action, the action against the fraudulent director is brought in the shareholder's name. There are two requirements that need to be satisfied before the court may grant leave to start a derivative action, namely:

- it is prima facie in the interest of the company that the action should be brought; and
- the complainant must have standing to bring the action, by showing that there has been "fraud committed against the minority" and the alleged wrongdoers are in control of the company.

The idea of "fraud on the minority" is a term of art here and is different from actual fraud under common law. It includes, for example, situations where the director misappropriates the company's money or opportunities, or receives bribes or benefits at the expense of the company.

4. OVERSEAS PARTIES IN FRAUD CLAIMS

4.1 Joining Overseas Parties to Fraud Claims

In order to bring a claim against overseas parties, it must be established that the Singapore court has a valid basis to assume jurisdiction over the overseas parties.

The Rules of Court prescribe specific bases for the Singapore court to assume jurisdiction over overseas parties, and in the context of fraud claims, the most often cited ground is that the overseas parties have assets located in Singapore, or that the defendant's actions have caused damage suffered either in whole or in part in Singapore.

Whether or not the Singapore courts assume extraterritorial jurisdiction will depend on the nature of the specific issue at hand. The Singapore Court of Appeal has held that the Singapore courts do not have jurisdiction to adjudicate on matters concerning immovable property located outside of Singapore. In a separate case, it was held that the Singapore courts can order a foreign individual to be subject to examination of judgment debtor proceedings if the foreign individual is so closely connected to the substantive claim that the Singapore court is justified in taking jurisdiction over him or her.

5. ENFORCEMENT

5.1 Methods of Enforcement

After a judgment is issued, the recovery of lost assets may still be frustrated as the fraudster may undertake efforts to make enforcement of the judgment difficult. For instance, the fraudster may seek to conceal or dissipate its assets, or may simply refuse to comply with the judgment order. There are various court remedies available to locate, preserve, and procure the assets of the fraudster.

Examination of the Judgment Debtor

Armed with a court judgment, the company may apply under Order 48 Rule 1 of the Rules of Court for an order for the Examination of Judgment Debtor against the fraudster. The fraudster would then be compelled to attend court to answer questions relating to his or her existing property, or property which may become available to him or her. The fraudster may also be compelled to produce any books or documents in his or her possession which are relevant to his or her assets.

Preservation of Assets

Freezing orders, as explained at **1.7 Prevention of Defendants Dissipating or Secreting Assets**, are also available as remedies to preserve the assets of the fraudster post-judgment,

pending execution. Given that a judgment has already been obtained, an application for a post-judgment freezing order requires only that there are grounds for believing that the debtor intends to dispose of his or her assets to avoid execution.

Writ of Seizure and Sale

Where it is known that properties belonging to the fraudster exist within the jurisdiction, a writ of execution may be issued under Order 46 of the Rules of Court for the properties to be seized by a public official and sold. The proceeds of sale will then be paid to the company in satisfaction of the judgment debt.

Garnishee Proceedings

Where it is known that the fraudster is owed debts by other persons, garnishee proceedings may be taken out under Order 49 of the Rules of Court. Provided that the debt is owned by the fraudster only, the court will issue an order for the garnishee (debtor) to pay the debt amount to the plaintiff, up to the value of the judgment amount. The most common targets of garnishee proceedings are banks in which fraudsters have deposited money.

Contempt Orders

As a measure of last resort, an application for a committal order may be taken out against the fraudster under Order 52 Rule 2 of the Rules of Court. This entails the threat of criminal sanctions against the fraudster to compel compliance with the judgment issued.

6. PRIVILEGES

6.1 Invoking the Privilege against Self-incrimination

The right to silence can be invoked when a person is asked to provide information that has a tendency to incriminate him or her. However, the fact that the answer or the document to be provided will expose the person to civil liability is generally insufficient to attract the privilege.

The right is therefore more commonly applied in criminal proceedings. In Singapore, the right to self-incrimination is not a constitutional right under the principles of natural justice. When summoned for an investigation, one must state what he or she knows about the facts and circumstances of the case, except that he or she is not required to disclose anything which he or she thinks might expose him or her to a criminal charge, such as admitting or suggesting that he or she did it.

At the same time, the court has the power under Section 116(g) of the Evidence Act to presume that evidence which could be and is not produced, would if produced, be unfavourable to the person who withholds it. As a result, courts have drawn adverse inference against a party who fails to produce documents or call crucial witnesses to testify at trial, both in civil and criminal proceedings.

In order for the court to draw adverse inference, there are two main requirements that need to be satisfied:

- there needs to be a substratum of evidence which establishes a prima facie case against the person against whom the inference is to be drawn. In other words, there must already be a case to answer on that issue before the court is entitled to draw the desired inference; and
- that person must have access to the information he or she is said to be concealing or withholding.

Note that in criminal proceedings, Section 261 of the Criminal Procedure Code expressly provides the Singapore courts with the power to

draw adverse inference from the silence of the accused for failing to mention any fact which he or she subsequently relies on in his or her defence.

6.2 Undermining the Privilege over Communications Exempt from Discovery or Disclosure

While communications between a lawyer and client attract legal advice privilege or litigation privilege, such communications can be stripped of their privileged status on the basis of "fraud exception".

In particular, Section 128(2) of the Evidence Act expressly provides that legal advice privilege will not apply to "any communication made in furtherance of any illegal purpose" or "any fact observed by any advocate or solicitor in the course of his [or her] employment as such showing that any crime or fraud has been committed since the commencement of his [or her] employment." The Singapore courts have held that litigation privilege is also subject to the same fraud exception.

The party seeking to lift privilege must at least show some prima facie evidence that the privileged communications were made as part of an ongoing fraud. When determining whether the "fraud exception" applies, the court will conduct a balancing exercise between the protection of privilege and the importance of preventing the commission of such fraudulent and/or criminal acts.

7. SPECIAL RULES AND LAWS

7.1 Rules for Claiming Punitive or Exemplary Damages

Generally, the Singapore courts have not been willing to award punitive damages in contract law, as the purpose of damages in contract law is to compensate the plaintiff for his or her loss, instead of punishing the wrongdoer. Even if fraud is established, the courts are reluctant to award punitive damages and depart from the general rule that punitive damages cannot be awarded for breach of contract.

Punitive damages may, however, be awarded for claims in tort, where the totality of the defendant's conduct is so outrageous that it warrants punishment, deterrence, and condemnation. The courts will also consider whether the defendant has already been punished by criminal law or through the imposition of a disciplinary sanction when deciding whether to award punitive damages. The overarching principle is that the courts will not make a punitive award when there is no need to do so.

7.2 Laws to Protect "Banking Secrecy"

Under Section 47(1) of the Banking Act, the bank is not allowed to disclose customer information to any other persons. However, the Banking Act also provides exceptions where disclosure is allowed, for instance, where the disclosure is necessary to comply with a court order, or to comply with a request made pursuant to written law to furnish information for the purposes of an investigation or prosecution of a suspected offence.

As such, there are recognised exceptions to the banking secrecy laws such as a Bankers' Trust Order (see **2.3 Obtaining Disclosure of Documents and Evidence from Third Parties**). The customer's information can also be provided to a police officer or public officer who is duly authorised to carry out the investigation or prosecution.

Rajah & Tann Singapore LLP is one of the few firms in the region with a dedicated Fraud, Asset Recovery, Investigations and Management (FICM) team that includes former prosecution lawyers and legal advisers to the Commercial Affairs Department of the Singapore police force. The FICM team builds upon the wealth of experience gathered by its partners in dealing with complex cross-border commercial fraud, cross-border asset recovery, white-collar crime, regulatory and compliance advice and insolvency as well as through its close collaborations with anti-fraud, anti-bribery and forensic-accounting professionals across a multitude of industries. The firm has acted in some of the most high-profile cross-border investigations seen in the region, notably, Lehman Brothers, MF Global, Wirecard's investigations into fraud allegations, the collapse of OW Bunker, and the Malaysian 1MDB scandal. Rajah & Tann Singapore is a member firm of Rajah & Tann Asia, a network of over 800 fee earners across ten jurisdictions, offering the reach and resources to deliver excellent service to clients, including in the Singapore-based regional desks focusing on Brunei, Japan and South Asia.

AUTHORS

Danny Ong is a partner at Rajah & Tann Singapore, where he specialises in complex international commercial disputes and investigations across a range of industries. In particular, in banking and finance, he has led cross-border disputes involving complex financial products, cryptocurrencies, insider trading, securitisation transactions, and money laundering. He is also known for his work in cross-border fraud and asset recovery investigations and litigation as well as in some of the largest and most complex insolvencies in the region. Danny has been recognised in these areas of expertise by international legal directories and publications. He is a lead advocacy trainer for the Singapore Institute of Legal Education and a founding director and vice president of the Turnaround Management Association (TMA) of Singapore and South-East Asia.

Jansen Chow is a partner at Rajah & Tann Singapore, where he covers a wide range of commercial matters, with a particular focus on disputes, often with challenging issues of law, including cross-border elements and foreign law. He has acted in a number of fraud and asset tracing matters, and has most recently acted for a conglomerate of 15 banks in pursuing Mareva injunctions and Norwich Pharmacal disclosure orders against a commodities trader for fraud claims of approximately USD100 million. This was, and remains, one of the largest fraud claims in Singapore.

Yam Wern-Jhien is a partner at Rajah & Tann Singapore. He is experienced in cross-border fraud and asset recovery cases, in particular, fraudulent e-commerce transactions, financing fraud, payment processing fraud, and cryptocurrency fraud. He has led and successfully obtained a number of freezing and proprietary injunctions and pre-action disclosure orders in aid of recovery actions in Singapore and in foreign jurisdictions, including the first known instance of the grant of a proprietary injunction over cryptocurrencies in Singapore. Wern-Jhien has also been involved in complex commercial disputes covering a wide variety of industries, including banking and financial services, construction, pharmaceutical, oil and gas, electronics, office supplies and hospitality.

Rajah & Tann Singapore LLP

9 Straits View #06-07
Marina One West Tower
Singapore 018937

Tel: +65 6535 3600
Email: info@rajahtannasia.com
Web: www.rajahtannasia.com

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA

Trends and Developments

Contributed by:
Danny Ong, Jansen Chow and Yam Wern-Jhien
Rajah & Tann Singapore LLP see p.18

Introduction

Finance fraud has been around since the dawn of commerce, with the first case reported as early as 300 BC. Developments in commerce and technology have seen fraud rear its ugly head repeatedly in different forms. Singapore, being a trading and financial hub, has inevitably seen its fair share of fraud occurring within or through its borders and network. Noticeably in recent years, there has been an upward trend of fraud incidents in two specific industries, namely commodities and cryptocurrency trading. In this article, we will explore how the fraud schemes came about, the difficulties faced in policing and recovery, as well as attempts by the Singapore government to address the issues.

Commodities Trading Fraud

Fraud in the commodities trading industry

The COVID-19 pandemic unearthed a spate of fraud cases in the commodities trading industry. In just under a year, fraud allegations have been levied against four commodities traders based in Singapore - namely Hontop Energy, Agritrade International, Hin Leong, and Zen Rock – who collectively leave their creditors facing potential losses amounting to billions of dollars.

The common thread in these incidents of fraud is the use of forged "transferable documents", which are essentially documents that entitle the holder to claim performance of the obligations indicated therein. For example, after Agritrade International collapsed with over USD1.5 billion in debt, it was reported that it had issued forged transferable documents to various lenders to secure multiple financing over the same goods. Similarly, the investigations by judicial managers of Hin Leong and Zenrock also pointed towards the use of forged transferable documents to secure duplicate trade financing over the same goods.

The impact of these fraud incidents cannot be overstated. Commodities trading operates on an international scale and is interconnected across various other industries. Fraud of such magnitude will inevitably see a loss of trust, increased cost and reduced competitiveness across countless businesses globally.

Asset tracing in cases of commodities trading fraud

In the above-mentioned examples of Hontop Energy, Agritrade International, Hin Leong, and Zen Rock, a substantial amount of time had passed before the fraud was discovered. As a result, by the time of the discovery, the fraud proceeds would likely have been dissipated in the form of payments to various parties, including other creditors, employees, and customers of the fraudulent commodities trader.

The commodities traders were subsequently placed in liquidation or some form of judicial management, where insolvency practitioners were appointed to replace the management of the company and tasked with leading the investigation and asset tracing efforts.

Claims have also been brought against the management of fraudulent commodities traders in their personal capacities. This method has been employed in the case of Hin Leong where the judicial managers, PricewaterhouseCoopers (PwC), have applied to freeze the assets of Hin Leong's founder (Lim Oon Kuin) and his two children. In the court papers filed in December 2020,

PwC sought orders to the effect that Lim Oon Kuin and his children shall not dispose or deal with any of their assets up to a sum of USD3.5 billion. Whether the personal assets of Lim Oon Kuin and his children are sufficient to meet the company's debt of USD3.5 billion remains to be seen.

Singapore's Electronic Transactions (Amendment) Bill

In a bid to combat, amongst others, commodities trading fraud, Singapore's Parliament passed the Electronic Transactions (Amendment) Bill (ETAB) on 1 February 2021, making Singapore the second country to adopt the United Nations Model Law on Electronic Transferable Record (MLETR) after the Kingdom of Bahrain.

The ETAB seeks to combat fraud by legally recognising electronic transferable documents which present a lower risk of forgery when compared to their paper counterparts. Clause 6 of the ETAB inserts sections 16A to 16S into Singapore's Electronic Transactions Act (chapter 88), which collectively ensure that electronic transferable documents are functionally and legally equivalent to paper transferable documents and are capable of being recognised as "documents of title". It is hoped that, with legislative support for the switch to electronic transferable documents, the commodities industry will adapt accordingly and join the fight against fraud.

Electronic transferable documents will be more difficult to forge because they utilise technologies which have authentication and traceability features at their core. For example, the authentication of electronic transferable documents is done almost instantaneously via digital signatures which are almost impossible to forge without access to the signor's device. This is far superior to the authentication process of paper documents, which involves verifying wet signatures and watermarks that can easily be forged with today's developments in reprography.

Furthermore, unlike their paper counterparts, electronic transferable documents also use technology that enables audit trails to be conducted. This allows all relevant parties to, at any time, review the progress of the transaction, identify the timing of any amendments, and determine by whom the amendments were made. Apart from bringing about greater convenience for all parties, this technology also facilitates forensic investigations in the event of a security breach.

That said, the fight against fraud in the commodities industry will require a concerted global effort and the ETAB alone will not be enough. As long as one party in the international supply chain continues to utilise paper documents, the risk of forgery will always subsist. Therefore, it is hoped that the rest of the world will proceed to enact similar legislation to encourage the adoption of electronic transferable documents. Doing so would not only reduce costs in cross-border trade, but would also be a significant milestone in the fight against fraud.

Cryptocurrency Trading Fraud

Fraud in the cryptocurrency trading industry

Although transactions in the cryptocurrency industry are generally secure as a result of blockchain technology, fraud can still occur in many other ways. For example, Singapore has seen an increased number of "cryptocurrency investment scams" where fraudsters persuade their victims to purchase cryptocurrency and transfer it to them for investment purposes. Some fraudsters achieve this by advertising false endorsements of their investment schemes by well-known local celebrities or esteemed politicians. This mode of fraud has gained sufficient traction in Singapore that the Monetary Authority of Singapore (MAS) and the Singapore police force have deemed

it necessary to issue public notices warning of such scams.

Another form of cryptocurrency fraud involves the use of fabricated cryptocurrencies, where fraudsters persuade their victims to invest in their own versions of cryptocurrency. A well-known example of this is the OneCoin Ponzi scheme which defrauded investors worldwide of billions of dollars. In exchange for fiat money, OneCoin gave its investors educational courses and tokens which could be used to mine OneCoins, an alleged form of cryptocurrency. These OneCoins could then be exchanged for a limited amount fiat currency on a private cryptocurrency exchange called Xcoinx, depending on how much one had invested. However, in reality, there was no blockchain technology involved and the OneCoins were eventually discovered to be worthless.

Although OneCoin was based in Bulgaria, its victims spanned multiple jurisdictions including the USA, Europe, China and even Singapore. In fact, two Singaporeans (Terence Lim Yoong Fook and Fok Fook Seng) were convicted last year for promoting OneCoin in Singapore and causing over 2,300 locals to be defrauded.

Asset tracing in cases of cryptocurrency trading fraud

Difficulty arises on the question of which jurisdiction disclosure orders should be sought from. This is because the entities that are likely to possess relevant information are cryptocurrency exchanges, which tend to be unregulated and not headquartered in any specific jurisdiction. For example, despite being the largest cryptocurrency exchange in the world in terms of trading volume, the location of Binance's headquarters is either a secret or non-existent. When asked about the location of Binance's headquarters at ConsenSys' Ethereal Summit in 2020, Binance's CEO (Zhao Changpeng) did not provide a definite location, and instead focused on Binance being a new type of organisation that did not need registered bank accounts or postal addresses. This issue will be particularly troublesome in cases involving large cryptocurrency exchanges with offices all over the world and in cases where the cryptocurrency exchange cannot be physically located.

Another practical problem that could arise is with regard to the identification of the stolen assets. As cryptocurrency fraudsters know that their transfers will be traced, they often arrange to conceal their ill-gotten gains by passing them through what is known as a "coin mixer". This software essentially breaks up the cryptocurrency into smaller amounts, sends them to be mixed with cryptocurrencies in thousands of other crypto-wallets, before finally depositing them in an account of the fraudster's choice. As one can imagine, tracing and identifying the stolen cryptocurrency would be extremely difficult after a coin mixer has been used due to the extensive mixing of the assets with other sources of cryptocurrency.

This is precisely why it is imperative to act with utmost urgency in cases of cryptocurrency fraud. Failing to do so only enables the fraudsters to further conceal the stolen assets. As such, the expeditious appointment of competent legal counsel and forensic teams to trace and recover these assets could mean the difference between a successful and an unsuccessful recovery.

Singapore's Payment Services Act

Singapore's Payment Services Act 2019 (No 2 of 2019) ("PS Act") came into force on 28 January 2020. One of its aims is to provide better protection of the public in the payment services sector, which includes the trading of cryptocurrencies.

In relation to the cryptocurrency industry, Section 6 of PS Act requires cryptocurrency exchanges

to apply for a licence before they are allowed to operate in Singapore, as they generally fall under the categories of an "e-money issuance service" and a "digital payment token service".

This licensing regime aims to reduce the incidents of cryptocurrency fraud in Singapore by imposing fraud-prevention obligations on licensed cryptocurrency exchanges. For example, the MAS has issued "Notice PSN03" pursuant to its powers under Section 102 of the PS Act, which imposes on cryptocurrency exchanges an obligation to report "any suspicious activities and incidents of fraud". Technology risk management obligations have also been imposed on licensed cryptocurrency exchanges in Singapore via "Notice PSN05", which include the requirement to implement safeguards to protect their customer's information from unauthorised access or disclosure, and to take steps to prevent and detect any cyber-attacks.

Many welcome the PS Act as a step towards regulating the opaque and high-risk cryptocurrency industry which has caused many to fall victim to fraud. While it remains to be seen whether the PS Act is effective in preventing cryptocurrency fraud, it is undoubtedly a first step in the right direction.

Conclusion

It is undeniable that fraud will continue to exist in our world and take on many forms as commerce and technology continue to develop. While fraud is certainly impossible to eradicate, measures can be taken to reduce its occurrence and mitigate its consequences. As much as governments have a duty to enact legislation and promote technology to combat fraud, legal practitioners should also be aware of the evolving nature of fraud and how best to recover the stolen proceeds for their clients. It is hoped that this article has provided information that will enable legal practitioners and their clients to better understand the trends and developments of fraud and asset tracing in Singapore today.

Rajah & Tann Singapore LLP is one of the few firms in the region with a dedicated Fraud, Asset Recovery, Investigations and Management (FICM) team that includes former prosecution lawyers and legal advisers to the Commercial Affairs Department of the Singapore police force. The FICM team builds upon the wealth of experience gathered by its partners in dealing with complex cross-border commercial fraud, cross-border asset recovery, white-collar crime, regulatory and compliance advice and insolvency as well as through its close collaborations with anti-fraud, anti-bribery and forensic-accounting professionals across a multitude of industries. The firm has acted in some of the most high-profile cross-border investigations seen in the region, notably, Lehman Brothers, MF Global, Wirecard's investigations into fraud allegations, the collapse of OW Bunker, and the Malaysian 1MDB scandal. Rajah & Tann Singapore is a member firm of Rajah & Tann Asia, a network of over 800 fee earners across ten jurisdictions, offering the reach and resources to deliver excellent service to clients, including in the Singapore-based regional desks focusing on Brunei, Japan and South Asia.

AUTHORS

Danny Ong is a partner at Rajah & Tann Singapore, where he specialises in complex international commercial disputes and investigations across a range of industries. In particular, in banking and finance, he has led cross-border disputes involving complex financial products, cryptocurrencies, insider trading, securitisation transactions, and money laundering. He is also known for his work in cross-border fraud and asset recovery investigations and litigation as well as in some of the largest and most complex insolvencies in the region. Danny has been recognised in these areas of expertise by international legal directories and publications. He is a lead advocacy trainer for the Singapore Institute of Legal Education and a founding director and vice president of the Turnaround Management Association (TMA) of Singapore and South-East Asia.

Jansen Chow is a partner at Rajah & Tann Singapore, where he covers a wide range of commercial matters, with a particular focus on disputes, often with challenging issues of law, including cross-border elements and foreign law. He has acted in a number of fraud and asset tracing matters, and has most recently acted for a conglomerate of 15 banks in pursuing Mareva injunctions and Norwich Pharmacal disclosure orders against a commodities trader for fraud claims of approximately USD100 million. This was, and remains, one of the largest fraud claims in Singapore.

Yam Wern-Jhien is a partner at Rajah & Tann Singapore. He is experienced in cross-border fraud and asset recovery cases, in particular, fraudulent e-commerce transactions, financing fraud, payment processing fraud, and cryptocurrency fraud. He has led and successfully obtained a number of freezing and proprietary injunctions and pre-action disclosure orders in aid of recovery actions in Singapore and in foreign jurisdictions, including the first known instance of the grant of a proprietary injunction over cryptocurrencies in Singapore. Wern-Jhien has also been involved in complex commercial disputes covering a wide variety of industries, including banking and financial services, construction, pharmaceutical, oil and gas, electronics, office supplies and hospitality.

Rajah & Tann Singapore LLP

9 Straits View #06-07
Marina One West Tower
Singapore 018937

Tel: +65 6535 3600
Email: info@rajahtannasia.com
Web: www.rajahtannasia.com

RAJAH & TANN ASIA
LAWYERS WHO KNOW ASIA