Contents

Introduction

Trade credit

Letters of credit and fraud exception – *Petrosaudi Oil Services (Venezuela) Ltd v Novo Banco SA (1) PDVSA Servicos SA (2) PDVSA Services BV (3)*
The English Court of Appeal has clarified a number of key features of Letters of Credit, including the "autonomy principle" and the scope of the fraud exception. The Court considered what evidence of fraud is required for a bank to legally withhold payment, and what is meant by the term "obligated to pay".

Singapore legal insurance update

Enforceability of general declaration clauses – condition precedent to liability
In the case of *Grace Electrical Engineering Pte Ltd v EQ Insurance Co Ltd* [2016] SGHC 233, the Singapore High Court had to determine the ambit and scope of such a general declaration clause to determine whether a breach of the "conditions" would entitle the insurer to avoid liability.

Cyber risks

Preventing and dealing with ransomware attacks – a legal and practical perspective
Recent cyber-attacks have highlighted the growing danger posed by ransomware extortion. Cyber insurance holds a role in handling and preventing a ransomware attack, but it is less clear whether making a ransom payment is lawful in Hong Kong.

Professional and financial risks

Aggregation revisited – AIG Europe Limited v Woodman & Ors
In *AIG Europe Limited v Woodman & Ors* [2017] UKSC 18, the UK Supreme Court considered the proper construction of the aggregation clause in the English Law Society's minimum insurance terms for solicitors in England and Wales. This decision is likely to be of considerable interest and relevance to Hong Kong and Singapore.

Medical malpractice

The medical indemnity insurance landscape in Singapore
A number of new entrants have emerged into the medical indemnity insurance market in Singapore for a number of reasons. With new key insurance providers, it seems that the market is becoming more competitive.

Letters of credit and fraud exception – *Petrosaudi Oil Services (Venezuela) Ltd v Novo Banco SA (1) PDVSA Servicos SA (2) PDVSA Services BV (3)*

Under a Letter of Credit once a compliant demand for payment has been made by a beneficiary, the issuing bank is obligated to make payment subject to very limited exceptions, such as the fraud exception. But what evidence of fraud is required in order for a bank to legally withhold payment to a beneficiary under a Letter of Credit and, where a beneficiary is required to certify that the buyer is "obligated to pay" the sums due under the underlying sales contract, what exactly is meant by the term "obligated to pay"?

These were the issues which the English Court of Appeal had to consider earlier this year in the case of *Petrosaudi Oil Services (Venezuela) Ltd v Novo Banco SA (1) PDVSA Servicos SA (2) PDVSA Services BV (3)* [2017] EWCA Civ 9). The ruling provides helpful clarification of a number of key features of Letters of Credit, including both the 'autonomy principle' and the scope of the fraud exception. For commercial entities regularly transacting on the basis of Letters of Credit, this serves as a welcome refresher.

This decision is not just of interest to the banks involved in issuing/advising/confirming negotiating or reimbursing Letters of Credit but also to insurers and reinsurers (both crime/fidelity and professional indemnity) of those banks and trade credit insurers (where Letters of Credit are often used to secure insured receivables).

The case

The claimants Petrosaudi entered into a contract with PDVSA under which Petrosaudi would provide drilling services to PDVSA in Venezuela. The drilling contract was subject to Venezuelan law and payment under the contract was guaranteed by an English Law standby Letter of Credit supplied by a Portuguese issuing bank. The parties entered into a long-running dispute in relation to various unpaid invoices and this dispute was submitted to arbitration. During the proceedings, Petrosaudi attempted to rely on a "pay now argue later" clause in the drilling contract and the arbitral panel ruled that, as this clause was incompatible with Venezuelan law, it was null and void. In light of this, PDVSA was not permitted under Venezuelan law to make payment under the drilling contract until the arbitration proceedings were concluded.

In advance of the final arbitral award, Petrosaudi sought to exercise its rights under the Letter of Credit by submitting a demand for payment of $129 million from the issuing bank. The Letter of Credit required that, when making this demand, Petrosaudi certify to the bank that PDVSA was "obligated to pay" the $129 million under the drilling contract which Petrosaudi duly did. The bank then indicated its intention to make payment under the Letter of Credit and, in response, PDVSA applied for an injunction seeking to restrain the bank from making payment on the basis of the fraud exception. Specifically, PDVSA argued that Petrosaudi had submitted the demand for payment under the LCs fraudulently as it had no honest belief that PDVSA was at that time obligated to pay under the drilling contract due to the finding of the arbitral panel. Petrosaudi opposed this view and sought a declaratory judgment that the bank was liable to pay.

The legal questions

The key questions for the court to consider were twofold:

- what was meant by the term "obligated to pay": did this mean only that PDVSA had a general liability to pay under the drilling contract or did it mean that PDVSA had an immediate obligation to pay now?, and
- dependent on the finding above, was Petrosaudi entitled to submit a demand for payment under the Letter of Credit or were its actions in doing so fraudulent?

The judgment

Overturning the High Court's judgement, the Court of Appeal held that the term "obligated to pay" did not require PDVSA to be under an immediate obligation to pay. Instead it could include the present situation where PDVSA had a liability to pay under the drilling contract but could not make payment while the arbitral proceedings were ongoing. When reaching this interpretation the court considered the context in which the words appeared; in particular the fact that they formed part of a Letter of Credit which was independent from the drilling contract, that the interpretation made good commercial sense (the availability of the Letter of Credit was of critical importance given PDVSA's payment history) and that it was not inconsistent with the finding of the arbitral panel.

The court held that the fraud exception requires the beneficiary to be "conscious of the falsity of what he was saying" or to have "no honest belief in, or reckless indifference to, its truth". The term "obligated to pay" could be interpreted in different ways and an incorrect legal interpretation of this term was not sufficient to constitute fraud for the purpose of the fraud exception. In light of this, the court ruled that Petrosaudi had been entitled to submit a demand for payment under the Letter of Credit and had not been acting fraudulently in doing so. It followed that the bank was ordered to pay the amounts demanded.

Commentary

This case reaffirms many key aspects of Letters of Credit, particularly:

- the "autonomy principle" – a Letter of Credit is autonomous and independent from the underlying transaction to which it stands as security. Accordingly, the bank's obligation to pay is not affected by a dispute between the parties to the underlying contract
- the fraud exception applies only in very narrow circumstances. This provides comfort to commercial sellers in that banks are only able to withhold payment under the fraud exception where it is clearly "established" or "obvious" that the beneficiary was involved in fraud relating to the transaction
- exceptions to the rule that an issuing bank must pay under a Letter of Credit are limited and often difficult to prove
- with pressure still on international trade/commodity prices and defaults still prevalent, banks involved in the associated Letter of Credit often get involved in disputes relating to payment of Letters of Credit. Crime/fidelity or professional indemnity insurers of banks involved in the Letter of Credit process will welcome this clarity as to a bank's duties in respect of a Letter of Credit
- trade credit insurers often have the benefit of a Letter of Credit in respect of insured receivables. The reaffirmation of the "autonomy principle" of the Letter of Credit will be reassuring albeit if there is a dispute (depending on the definition of "dispute" within the respective trade credit policy), the claim for the outstanding receivable may not be covered until the dispute is resolved unconditionally in the insured's favour. This is a reminder for trade credit insurers to concentrate on the drafting of their disputes definition/clauses.

Geraldine Bourke
Legal Director
+65 6422 3041
geraldine.bourke@rpc.com.sg

Chris Neilson
Senior Associate
+65 6422 3043
christopher.neilson@rpc.com.sg

Enforceability of general declaration clauses – condition precedent to liability

Introduction

It is a common feature of insurance policies to contain a general declaration clause specifying that compliance with some, if not all, of the obligations as contained in the policy, by the insured, would be a condition precedent to liability of the insurer.

In the case of *Grace Electrical Engineering Pte Ltd v EQ Insurance Co Ltd* [2016] SGHC 233, the Singapore High Court had to determine the ambit and scope of such a general declaration clause to determine whether a breach of the "conditions" would entitle the insurer to avoid liability.

Facts

At the material time, Grace Electrical Engineering Pte Ltd ("Grace Electrical") was the occupier of a building ("Unit 141") which was used both to carry out its business operations and a dormitory for its foreign workers. There were electrical cooking appliances, fans and refrigerators in the backyard for the workers' use and the workers cooked their meals in Unit 141.

A fire broke out in Unit 141 on 6 September 2012, which spread to an adjoining building occupied by Te Deum Engineering Pte Ltd ("Te Deum"). In a separate case, the Singapore High Court found Grace Electrical liable in negligence for the fire damage to the building occupied by Te Deum.

After the outbreak of the fire, the Singapore Civil Defence Force ("SCDF"), charges were brought against Grace Electrical under the Fire Safety Act ("FSA") in relation to the unauthorised use of Unit 141 for storage and accommodation purposes and for carrying out unauthorised fire safety works. A total of 8 charges were levelled against Grace Electrical who eventually pleaded guilty to 5 of these 8 charges.

In 2014, Grace Electrical was sued for fire damage by Te Deum Engineering ("Te Deum") and was found liable in negligence. Grace Electrical then sought an indemnity under a public liability policy issued by EQ Insurance ("the Policy").

The terms of the Policy

The main issue before the High Court pertained to the construction of inter alia 3 general conditions in the Policy, namely general condition 4 ("GC 4"), general condition 9 ("GC 9"), and general condition 13 ("GC 13"). GC 4 and GC 9 were to be read with GC 13. These general conditions provided as follows:

- GC 4 provided that Grace Electrical would not repudiate liability or make any admission, offer or promise in connection with any accident or claim without the insurer's consent.
- GC 9 provided that Grace Electrical would exercise reasonable care that all statutory requirements and regulations imposed by any public authority are duly observed and complied with.
- GC 13 provided that the due observance of the terms of the Policy, insofar as they relate to anything to be done or not to be done by Grace Electrical, shall be conditions precedent to any liability of the insurer to make any indemnification under the same.

Effect of the general declaration clause

The High Court upheld the enforceability of the general declaration clause i.e. GC 13, and held that compliance with GC 4 and GC 9 were in fact conditions precedent to the insurer's liability under the Policy. Furthermore it held that Grace Electrical had breached GC 9 as it had been reckless in its violations of the FSA.

In ascertaining whether GC 4 and GC 9 were in fact conditions precedents to the insurer's liability, the High Court inter alia took into account the following factors:

- **Fairness** – the Court held there would be no blanket application to such clauses but that the "effect of a general declaration clause like GC 13 (that declares a group of terms to be conditions precedent) must be examined with each specified clause in a policy that is purported to be a condition precedent to liability". Such clauses should be construed fairly to give effect to the object for which they were inserted, but at the same time so as to protect the insured from being trapped by obscure or ambiguous phraseology.

- **Workability** – an important factor to be considered would be the workability of the contractual obligation as a condition precedent to liability as it would not be possible to give effect to such a clause if to do so would give rise to absurdity. In this regard, whilst the usage of the label "condition" or "condition precedent" would be regarded as a relevant factor, this was not decisive of the contractual term's legal effect, especially when such a label is attached generally to a number of terms of different nature.
- **Purpose** – the purpose of the relevant condition or that of the policy itself would also be a relevant factor to be considered in construing such clauses.
- **Ambiguity** – The contra proferentum rule, where an ambiguity in a document is resolved against the person who prepared it, is particularly pertinent in insurance policies because these policies are invariable drafted by experts for the benefit of insurers. In this regard, the construction of a general declaration clause would also be dependent on whether there was ambiguity in the said clause necessitating the application of the contra proferentum rule.

Comments

This decision is good news for insurers as it affirms the courts willingness to give effect to such general declaration clauses.

However, given that such clauses could be fairly onerous with any breach resulting in severe consequences, the ambit, scope and effect of such clauses will be determined on a case by case basis. In doing so, the courts will adopt a pragmatic and balanced approach, favouring substance over form.

Allister Tan
Senior Associate
+65 6422 3025
allister.tan@rpc.com.sg

Preventing and dealing with ransomware attacks – a legal and practical perspective

The recent "WannaCry" and "Petya" cyber-attacks have sent shockwaves through the global business community, highlighting the growing danger posed by ransomware extortion. These attacks involve the use of malicious software to encrypt the victim's data, blocking access to it and threatening to publish or delete it unless a ransom is paid. This article discusses how to handle and prevent a ransomware attack, focusing in particular on whether making a ransom payment is lawful in Hong Kong and on the role of cyber insurance.

The legality of ransom payments

It is understandable that some victims may be tempted to risk making the ransom payment, especially under time pressure. However, in many cases, it is doubtful whether it is worthwhile to make a ransom payment; there is a risk that the hacker may fail to release the data even after receiving the ransom, and paying a ransom might encourage repeat attacks by indicating that the victim is a "soft target". A further issue to consider, however, is whether a business making a ransom payment is acting lawfully in doing so. This not only concerns the victims, but also their insurers.

In summary, there is currently no specific legislation under Hong Kong law, or generally-applicable international law, which makes ransom payments illegal. There is also no duty on ransom payers to report such incidents to the Hong Kong Police (although the Police encourage them to do so).

In Mansefield AG v Amlin Corporate Member Ltd [2011] EWCA Civ 24, a case which involved the seizure of a vessel and its cargo and crew off the coast of Somalia by pirates, the common law position on whether the payment of a ransom is lawful was clarified by the Court of Appeal of England and Wales. An argument was raised that the ransom payment was unlawful since it was contrary to public policy to reward piracy.

The Court of Appeal rejected this argument, concluding that: "...there is no universal morality against the payment of ransom, the act not of the aggressor but of the victim of piratical threats, performed in order to save property and the liberty or life of hostages. There is no evidence before the court of such payments being illegal anywhere in the world. This is despite the realisation that the payment of ransom...encourages the incidence of piracy for the purposes of exacting more ransoms. (Perhaps it should be said that the pirates are not classified as terrorists. It may be that the position with regard to terrorists is different.)"

As for the court's observation that the public policy position with regard to terrorists could be different, this currently has limited relevance to ransomware attacks in Hong Kong. Section 7 of the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575) provides that a person must not provide or collect any property with the intention or knowledge that such property will be used to commit any terrorist acts; however, to date, there is no known connection between ransomware attacks in Hong Kong and terrorism (and even if there were, the victim may be unaware of it). It is therefore unlikely that a ransom payment made in response to a ransomware attack would fall within the scope of this offence.

Incidentally, the UK's Counter-Terrorism and Security Act 2015 introduced a new offence prohibiting insurers from making any reimbursement of ransom payments made by the insured to persons involved or suspected to be involved in terrorism. It remains to be seen whether Hong Kong will adopt a similar provision.

Litigation exposure for data breaches and data loss

Businesses suffering from ransomware attacks may face potential claims arising from data breaches or loss of data.

Under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), a "data user" shall comply with the data protection principles covering various aspects of "personal data". Principle 4 requires data users to take all practical steps to protect personal data against unauthorised or accidental access, processing, erasure, loss or use.

Those steps may include the use of secure computer software. For example, in the case of WannaCry, the hackers took advantage of a security flaw in the Microsoft Windows operating system. Microsoft had issued security patches for the more recent versions of Windows in order to address this vulnerability, but not all users had installed the patch. Of further concern was the vulnerability of the 16-year-old Microsoft Windows XP, for which Microsoft had stopped releasing security patches in April 2014. Despite its age, Windows XP has continued to be used widely. If hackers gained access to or destroyed personal data stored on a business's computer system as a result of its failure to update the operating system used on its computers or to download and install security patches when available, the business could be held to have failed to take adequate steps to prevent the incident, in contravention of Principle 4.

In addition, section 66 of the PDPO provides that any person suffering damages as a result of such contravention is entitled to claim compensation from the "data user". Victims therefore face potential exposure to civil claims from parties affected by damage to, disclosure of or loss of personal data, which may include their employees, clients and trading partners.

Cyber insurance

The Hong Kong Productivity Council recently reported a 23% rise in security incidents in Hong Kong in 2016 compared with 2015. Among the 6,058 incidents, malware cases (including ransom attacks) powered the surge, with the number of reported incidents increasing by 247%. In this context, cyber insurance stands to play an increasingly important role. Although policy terms vary significantly, policies generally provide coverage for costs connected with ransomware attacks, for example:

- **ransom payment** – usually a ransom is not paid up-front by the insurer; once the threat is over, the insurer will reimburse the policyholder for the ransom up to a certain amount
- **costs of data restoration** – victims will commonly consult computer specialists for assistance with decryption of the files or restoration from backups
- **loss of revenue due to business interruption** – typically, there must be a direct causal relationship between the ransomware attack, business interruption and the loss of revenue
- **costs of forensic investigation** – forensic investigations are usually required to determine the scope of the attack and the files which have been lost or encrypted
- **third party liability** – defence costs and civil damages arising from third party liability claims (eg customers and suppliers) arising out of a cyber incident may be covered, such as security and data breaches, defamation, breach of privacy and negligence claims.

Given the potentially broad range of risks covered, great care should be taken when drafting and reviewing policy wording. Areas particularly ripe for disputes, and which may be affected by the policy wording, include causation, the date on which the loss is deemed to have been suffered, the timeliness and proportionality of the insured's response, and the adequacy of the insured's cyber security measures

Guidance from regulators on reducing cyber risks

Part of an organisation's risk mitigation strategy should involve the adoption of adequate cyber security measures, failing which insurance cover may in some cases be denied (in some circumstances, directors and officers could also be exposed to personal liability). In response to the alarming proliferation of the WannaCry ransomware, on 15 May 2017 the Securities and Futures Commission published a circular[1] to alert all licensed corporations to the risk of ransomware attacks and suggested the following measures:

- apply the latest security update to your computers and network devices
- install and properly set up a firewall or broadband router for connecting your devices to the internet
- perform offline backup (ie backup on another storage device, disconnected after backup)
- avoid opening links and attachments in any suspicious emails
- avoid connecting any computer or device to your office network before proper security verification, and
- ensure that suitable antivirus/internet security software is installed and regularly updated.

Finally, the circular states that business entities are expected to evaluate the effectiveness of their cybersecurity controls critically and to seek advice from external experts if necessary.

The circular's recommendations are relevant not just to licensed corporations but also to a wide range of other organisations, including those not subject to industry-specific regulatory oversight. Also of relevance are the numerous circulars on cyber security in general issued by the SFC, HKMA and the Privacy Commissioner.

The security measures recommended in such circulars may, however, appear to many businesses to be prohibitively expensive to implement; proportionality is therefore key, and lawyers can assist in advising on what measures are likely to satisfy the applicable regulators as adequate for the organisation in question.

1. See http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC26

Conclusion

The recent growth in the number and scale of cyber-attack incidents has raised significant IT security issues across various industries in Hong Kong and across the world. Businesses should therefore be advised to keep a close eye on the latest technological developments and take all reasonable steps to protect their IT systems from such an attack.

However, the reality is that no system can be entirely invulnerable. Insurance therefore has an important and growing role to play in this area. There is an opportunity for insurers to work with insureds in implementing appropriate response plans to mitigate the potential losses resulting from ransomware attacks; such response plans should include the coordination of urgent assistance from lawyers and technical experts well versed in the field.

Ben Yates
Senior Associate
+852 2216 7169
ben.yates@rpc.com.hk

Aggregation revisited – *AIG Europe Limited v Woodman & Ors*

Introduction

Aggregation clauses are a common feature of professional liability insurance policies and can have a substantial impact on the amount of damages that an insured may be able to recover from its insurers. In *AIG Europe Limited v Woodman & Ors* [2017] UKSC 18, the UK Supreme Court considered the proper construction of the aggregation clause in the English Law Society's minimum insurance terms for solicitors in England and Wales, providing helpful clarification on how such clauses are to be interpreted.

Compared with the likes of England, insurance is still very much a developing body of law in Asia, and courts across the region continue to look to other jurisdictions for guidance on interpretation and construction of policy terms and conditions. While the courts in Hong Kong and Singapore have yet to consider a number of contentious areas of insurance law, including aggregation, this decision should be of considerable interest and relevance in the region.

Purpose of aggregation wording

The concept of aggregation is to enable two or more separate losses, which are both covered by an insurance policy, to be treated as a single loss for deductible or other purposes where they are linked by a unifying factor of some kind. It is the nature of the unifying factor which causes the most debate and, in each case, the legal test depends on the precise wording used to describe that which links the claims.

Where the description of the unifying act or event is narrow and specific, it will be more difficult to aggregate the claims, but where wide and general words are used, the courts can more readily find that the claims should aggregate. Whether the outcome benefits the insured or the insurer will often depend on the size and scale of the losses claimed. For example, an insured can benefit from only having to pay one deductible in respect of several linked claims, leaving the balance to be paid by the insurers (whose overall exposure is also capped). Alternatively, if the insured has to pay several deductibles, insurers may experience little or no outlay.

Facts

Midas, an international property development company, instructed a firm of solicitors ("ILP") to devise a mechanism for financing the development of two holiday resorts in Turkey and Morocco. IPL set up: (i) a scheme whereby IPL held investors' funds in an escrow account; and (ii) a trust for each development, to hold security for the investors over the land to be purchased, with the solicitors as the initial trustees.

The developments failed and Midas was wound-up. Legal proceedings were brought by 214 investors against ILP, claiming losses in excess of £10 million. It was alleged that ILP had released investor funds to the developers in breach of the terms of the underlying purchase and loan agreements, and without ensuring that adequate security was in place.

IPL sought indemnity from its insurer, AIG.

Dispute

The relevant professional indemnity policy provided for a £3 million limit of liability per claim. It also permitted the aggregation of claims "arising from similar acts or omissions in a series of related matters or transactions".

In March 2014, AIG issued proceedings against the insured solicitors seeking a declaration that all of the investors' claims constituted a single claim under the Policy or, alternatively, that each development constituted a separate claim, each with a single limit of indemnity.

The trustees of the two trusts established for each of the projects joined in the proceedings and, together with the insured, contended that the claims could not be so aggregated, with the result that the losses claimed should be recoverable in full.

Previous interpretations

At first instance, Teare J in the London Commercial Court accepted that the claims arose from similar acts or omissions, but rejected the argument that the claims were in "a series of related matters or transactions". He interpreted those words as referring to transactions that were related in the sense that they were conditional or dependent on each other. Since the transactions were not mutually dependent, it was held that they were not "related" such that the investors' claims did not aggregate. AIG appealed.

The English Court of Appeal adopted a different approach, having found Teare J's interpretation unduly narrow. It rejected the contention that the transactions had to be dependent upon one another in order to aggregate, and introduced the test that there must be some "intrinsic relationship" between the matters or transactions in order for aggregation to occur, rather than some external common factor (such as that the transactions or matters were conducted by the same solicitors, or related to the same geographical area).

The Court of Appeal remitted the case to the Commercial Court for determination. Again, AIG appealed.

UK Supreme Court's decision

The Supreme Court unanimously allowed AIG's appeal, rejecting both the intrinsic link test applied by the Court of Appeal and the inter-dependence test adopted by the Commercial Court. Lord Toulson gave the leading judgment, with which all agreed.

The Supreme Court held that, in determining whether the transactions were related was "an acutely fact sensitive exercise" and the application of the aggregation clause should be considered "in the round", rather than from the point of view of the parties to the insurance contract. This particular policy had been set by the Law Society, which, as a regulator, was seeking to balance protection of the public against the cost and availability of insurance for practitioners.

Lord Toulson described the test of whether the transactions were 'related' as requiring "some inter-connection between the matters or transactions, or in other words they must in some way fit together".

With this in mind, it was necessary to start by identifying and understanding the relevant matters or transactions. The relevant transactions in this case involved an investment in a particular development scheme under a contractual arrangement of which the trust deed and escrow agreement were part and parcel. The transactions were therefore connected in significant ways due to the shared objective of the underlying development project: the members of each group invested in a common development and were participants in a standard scheme and co-beneficiaries under a common trust. As such, the claims concerning each group of investors fell to be aggregated.

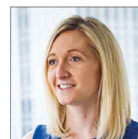
However, the court was not persuaded to aggregate the claims of one group of investors with those of another. The transactions concerned two separate developments (one in Morocco and one in Turkey), which were not connected: they related to different sites, and the different groups of investors were protected by different deeds of trust over different assets. That the claims bore "striking similarities" was not enough to render them "related" for the purpose of the aggregation clause.

Comment

This decision confirms that aggregation remains firmly a fact specific exercise of judgment and that construction of these clauses is not to be approached with any predisposition towards either a narrow or broad interpretation. This is reflective of the fact that aggregation clauses can operate in favour of either party and, at the time that the policy is drafted, neither party to the contract knows which side of the argument they might find themselves on.

That said, Lord Toulson's reasoning plainly provides support for a broader, common sense approach to construction of aggregation clauses, where the concept of what is "related" should not be qualified by any requirement that the matters and transactions share an "intrinsic link" or are inter-dependent. In this case, relatedness was assessed by considering the manner in which the transactions "fitted together", which would seem an easier test to understand and apply.

While the case remains confined to its specific facts, the overall approach is to be welcomed by professional indemnity insurers and policyholders alike, and not just in England and Wales; given the general principles involved, the judgment will be of interest to anyone transacting insurance business in civil law jurisdictions in the region. Indeed, the judgment of the UK Supreme Court is persuasive authority in common law jurisdictions (such as Hong Kong and Singapore), and in those jurisdictions that are principally common law (such as Malaysia). Unless and until the courts in Asia (with Hong Kong and Singapore being the most likely candidates) are asked to address this specific issue themselves, aggregation clauses found in professional indemnity policies across the region stand to be construed in a similar vein.



Carmel Green
Senior Associate
+852 2216 7112
carmel.green@rpc.com.hk

The medical indemnity insurance landscape in Singapore

Historically there have been a small number of providers monopolising the medical indemnity insurance market in Singapore. Recently, however a number of new entrants have emerged including (most recently) Jardine Lloyd Thompson ("JLT") which launched its Medical Practitioner's Indemnity product in July 2017. Along with Aon Singapore Pte Ltd ("Aon"), which entered the market in May 2015, this appears to pave the way for a more competitive insurance landscape. This article considers some of the reasons for this change and provides a summary of the key insurance providers in the Singapore market.

A history of medical indemnity insurance in Singapore

The history of medical indemnity insurance in Singapore has been far from uneventful. Historically there have been two main players – Medical Protection Society ("MPS"), which offered occurrence-based cover, and NTUC Income ("NTUC"), which offered claims-based cover. A number of practitioners were also previously covered under policies provided by the Australian medical defence organisation, United Medical Protection ("UMP"). However in 2001, following a landmark medical negligence case in Australia (and subsequent payout of A$11million) UMP collapsed leaving their Singaporean members scrambling for tail cover with MPS and NTUC.

In 2015 MPS abruptly announced that it was moving its obstetrics indemnity cover from occurrence-based to claims-based for all members of the Obstetrical and Gynaecological Society of Singapore (OGSS). This resulted in widespread concern that the increasing cost of cover for many practitioners (for example due to the need to buy tail cover on retirement) could cause them to move to other areas of medicine or to leave the profession altogether. Whilst this movement does not appear to have occurred, it is clear that some other providers (namely Aon) have followed the trend set by MPS by limiting the type of cover available for obstetricians and gynaecologists. This is discussed further below.

Towards a more competitive market?

In recent years, the medical indemnity insurance market has begun to expand with the arrival of two new providers – Aon and JLT. This change can largely be explained by the increasingly litigious climate for medical practitioners in Singapore. According to the Straits Times, claims against doctors recorded a 90% rise from 2006 to 2011. Further, according to the Straits Times, between 2013 and 2016, 34 medical negligence suits were filed with the Supreme Court (involving a potential total of at least $8.5 million in claims) and another 23 medical negligence cases were filed in the State Courts during the same period.

In light of the increasing appetite amongst claimants for bringing proceedings against their medical practitioners, the need for medical indemnity insurance is now more keenly felt. As a result, there is increasing business opportunity for insurance providers who are now finding more traction within the medical industry for such products.

Two further developments look set to continue the increase in the number of claims against medical practitioners in Singapore and which might result in further insurance providers entering the fold. First, there has been speculation that the recent judgment in *Hii Chii Kok v London Lucien Ooi* [2017] SGCA 38 (which introduces a new three-stage, "patient-centric" test[2] and higher duty of care for doctors advising patients of their choices and the risks involved in treatment) might lead to increased litigation. Secondly, with the growing middle class in Asia increasingly searching for the best healthcare and often travelling to Singapore for such treatment, Singaporean doctors now also face a risk of claims from foreign patients. Awards for medical negligence to date have been relatively modest (albeit that awards for negligence in general appear be getting higher); this is ripe for change with more foreign patients seeking help in Singapore.

The providers

There are currently four key providers of medical liability insurance in Singapore – MPL, NTUC, Aon and JLT.

MPS

The oldest of the current providers (having operated in Singapore for over 40 years), MPS offers a variety of memberships including occurrence-based, claims-based and group membership coverage.

MPS's claims-based protection for obstetricians and gynaecologists provides cover up to a discretionary limit of S$15 million per year of membership. MPS also provides "extended reporting benefits" ("ERBs") offering protection to practitioners in retirement. These ERBs can be purchased in one payment to cover one's whole retirement and the cost is determined on an individual basis.

MPS's occurrence-based protection applies to all other medical practitioners and responds to claims that arise even after a practitioner has left MPS membership.

2. This test has since been restated in two subsequent disciplinary cases brought by the Singapore Medical Council against Dr Ang Peng Tiam and Dr Chia Foong Lin.

NTUC

NTUC offers occurrence-based coverage with a maximum limit of indemnity set at S$5million for any one incident or any one year period of insurance. Premiums are calculated according to medical field with "Obstetric Risk" attracting the largest premium of S$31,351.00 and "Low Risk" practices (such as dermatology and paediatrics) attracting a premium of S$1,658.50.

Aon

Aon entered the market in May 2015 and offers occurrence-based cover ("Singapore Medical Indemnity" ("SMI")) underwritten by The Medical Professional Liability Company ("MPLC"), on behalf of certain Lloyd's Underwriters, London. Significantly, Aon insures all junior doctors in Singapore's restructured hospitals under Ministry of Health Holdings (MOHH). Aon offers a choice of indemnity limits up to a maximum of S$15million in the aggregate for all claims arising for treatment in the one year policy period. For Obstetricians, SMI cover is restricted - it is currently only available for non-hospitalisation treatment or for hospitalisation treatment carried out in four named hospitals.

JLT

The most recent entrant to the medical indemnity insurance market, JLT's Medical Practitioners Indemnity ("MPI") scheme was launched in July 2017. In Malaysia, JLT offers medical indemnity cover underwritten by Pacific & Orient Insurance Co. Bhd who are supported and backed by the international insurance group, Allied World. At the time of writing, there was limited publicly available information about JLT's Singapore MPI offering.

Conclusion

The structure of the medical indemnity insurance market in Singapore appears to be shifting; there is now a wider range of providers than ever before offering a mixture of occurrence-based and claims-based cover. Having said this, as things currently stand, the cover offered by the four key providers appears to be relatively uniform. However, in an increasingly litigious environment it is plausible that the medical indemnity insurance market may become increasingly competitive, resulting in lower premiums and increased consumer choice and purchasing power amongst medical practitioners. In such an environment, practitioners are more likely to be able to select a provider based on the type of cover offered, premium and limit of indemnity that is most appropriate to their area of medical specialism. As the likes of Aon and JLT become more established, and with the possibility that further new providers will enter the market, it remains to be seen just how and whether this movement will continue to shake up the sector.

Rachel Tan
Special Counsel
+65 6422 3011
rachel.tan@rpc.com.sg

Asia insurance contacts

Hong Kong

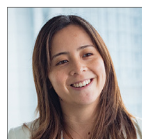
David Smyth
Senior Partner (Asia)
+852 2216 7100
david.smyth@rpc.com.hk

Antony Sassi
Partner
+852 2216 7101
antony.sassi@rpc.com.hk

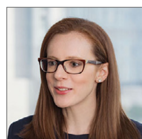
Carmel Green
Senior Associate
+852 2216 7112
carmel.green@rpc.com.hk

Ben Yates
Senior Associate
+852 2216 7169
ben.yates@rpc.com.hk

Samuel Hung
Associate
+852 2216 7138
samuel.hung@rpc.com.hk

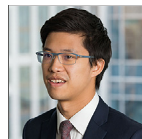


Rebecca Wong
Senior Associate
+852 2216 7168
rebecca.wong@rpc.com.hk



Hannah Fletcher
Registered Foreign Lawyer
+852 2216 7159
hannah.fletcher@rpc.com.hk

David Kwok
Associate
+852 2216 7114
david.kwok@rpc.com.hk



Adrian chang
Associate
+852 2216 7175
adrian.chang@rpc.com.hk

Singapore

Mark Errington
Partner
+65 6422 3040
mark.errington@rpc.com.sg

Iain Anderson
Partner
+65 6422 3050
iain.anderson@rpc.com.sg

Rachel Tan
Special Counsel
+65 6422 3011
rachel.tan@rpc.com.sg

Geraldine Bourke
Legal Director
+65 6422 3041
geraldine.bourke@rpc.com.sg

Summer Montague
Senior Associate
+65 6422 3042
summer.montague@rpc.com.sg

Chris Neilson
Senior Associate
+65 6422 3043
christopher.neilson@rpc.com.sg

Grant Pilkington
Senior Associate
+65 6422 3051
grant.pilkington@rpc.com.sg

Allister Tan
Senior Associate
+65 6422 3025
allister.tan@rpc.com.sg

Nazirah Kairo Din
Associate
+65 8798 1432
nazirah.kairodin@rpc.com.sg

17540