ALLEN & OVERY

November 2018

Litigation and Dispute Resolution

Review

Contents

Amy Edwards
Litigation – Senior Professional Support Lawyer – London

Contact
Tel +44 20 3088 2243
amy.edwards@allenovery.com

Antitrust

FIRST UK FOLLOW-ON CARTEL DAMAGES RULING

BritNed Development Ltd v ABB AB and ABB Ltd [2018] EWHC 2616 (Ch), 9 October 2018

The UK High Court ordered Swiss engineering company ABB to pay Anglo-Dutch power-grid joint venture BritNed just over EUR11.5 million in damages in a follow-on action relying on the European Commission's underground and undersea power cables cartel decision. The amount awarded is significantly smaller than the EUR180 million initially claimed, but the case is important in being one of only a handful of UK court judgments to date that have awarded private damages for harm suffered as a result of a breach of antitrust law.

The case stems from a 2014 decision by the European Commission (**EC**) which found that, between 1999 and 2009, ABB and ten other companies had been involved in a global cartel in the underground and submarine high-voltage power cable sector, by bid-rigging, market sharing and exchanging competitively sensitive information.

BritNed was a customer of ABB during the cartel period, following the negotiation and award of a cable supply contract to ABB for the construction of the BritNed Interconnector, an electricity submarine cable system connecting the UK with mainland Europe.

In 2015, BritNed issued proceedings against ABB, claiming it had suffered loss and damage in excess of EUR180 million as a result of the cartel and its operation.

BritNed claimed for three types of loss:

- **Overcharge Claim**: as a result of the cartel, it had paid more for the cable than it otherwise would have done;
- **Lost Profit Claim**: absent the cartel, it would have bought a cable with higher capacity which would have generated higher profits than the cable actually purchased; and
- **Compound Interest Claim**: compound interest on the basis that, as a result of the overcharge, it had incurred higher capital costs in commissioning the Interconnector than would otherwise have been the case under competitive conditions.

ABB did not deny participating in the cartel but argued that the cartel had had no effect on pricing or the choice of cabling and so BritNed had suffered no loss or damage. Alternatively, ABB argued that any damages fell to be assessed in light of the regulatory cap imposed on BritNed's earnings (the **Regulatory Cap Claim**).

Overcharge claim allowed in part

The court held that an overcharge had to be assessed as the difference between the price actually agreed between the parties and the price that a claimant would have agreed, whether with the defendant or with a rival provider, had the cartel not existed.

On the evidence, the court found that there had been no overcharge. BritNed had been able to put commercial pressure on ABB during the contractual negotiations, for example, through comparing value and costs with previous projects and the threat that the project would not go ahead if the price was too high. It was also important that the ABB individuals involved in the negotiations were unaware of the cartel's existence. The court found that the costings had been compiled honestly and competently with a view to putting forward a competitive bid.

"Baked-in inefficiencies" in cable design

Even though there was no "deliberate" overcharge, the court held that ABB's position in the cartel had allowed it to maintain "baked-in inefficiencies" in its cable design when compared to its competitors and that the cost of these inefficiencies had been passed on to BritNed.

The court stated that "had there been a properly competitive environment, ABB would have faced technical solutions from others", which would have resulted in ABB either cutting costs or losing the contract.

The court found that there was an overcharge to BritNed arising from this inefficiency and ordered ABB to pay just over EUR7.5 million.

Cartel savings

The court considered the internal savings ABB was ableto achieve as a result of not having to compete with its co-cartelists and ordered ABB to pay a further EUR5.5 million for these in respect of the BritNed project.

No lost profits

The Lost Profit Claim was dismissed as the evidence showed that, even in the absence of the cartel, BritNed would still have chosen the same power cable at the same price, thereby achieving the same profit.

No compound interest

The court dismissed BritNed's claim for compound interest. As BritNed was funded entirely through shareholder equity, through its parent companies, it had not incurred any additional costs from having to raise the additional capital. Further, the parent companies were not party to the proceedings. The court held it was "fundamentally wrong" to calculate interest by reference to the "hoped-for profit" of the parent companies. BritNed was, however, entitled to simple interest.

Regulatory Cap not relevant to damages claim

The court held that damages did not have to be assessed in light of the regulatory cap on BritNed's earnings as, following an exemption granted to BritNed in 2007, this cap would only bite after 25 years. The court held that even if, in future, BritNed made profits it would not have made but for the overcharge, in excess of the cap, it would still be entitled to recover the full amount of the overcharge. Under the regulatory regime, excess profits have to be used either to create further capacity expansion or to fund the regulated transmission networks in the UK and the Netherlands. Excess profits were not retained by BritNed and therefore it would not benefit from these damages by way of excess profit.

However, the court also held that, given the regulators were not party to the proceedings, it was not appropriate for it to determine the true effect of the exemption and so asked BritNed to provide an undertaking to treat damages as if they were subject to the cap in order to avoid over-compensation. Following a refusal by BritNed, the court, in a supplemental judgment, reduced the award for damages by 10% to just over EUR11.5 million.

COMMENT

The ruling is a clear reminder that companies granted immunity or leniency from regulatory fines can still, and do, face damages actions by third parties. Companies should therefore consider their potential liability when carrying out a risk assessment of a prospective immunity or leniency application.

With the proliferation of antitrust damages actions being lodged with the UK Courts, the importance of having a robust antitrust compliance programme in place is evident. On the flip side, for companies which believe they have suffered loss as a result of a breach of antitrust laws, the opportunity for redress is not just theoretical.

The court granted both parties permission to appeal.

Sophie Walker
Associate
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 4189
sophie.walker@allenovery.com

Crime

CYBERCRIME – REMEDIES AGAINST UNKNOWN HACKERS

CMOC Sales & Marketing Ltd v Person Unknown & 30 ors [2018] EWHC 2230 (Comm), 26 July 2018

The English High Court will adopt flexible and innovative approaches to help victims of cybercrime obtain remedies against defendants who are either unknown or refuse to engage in proceedings. The court confirmed its jurisdiction to grant world-wide freezing orders against persons unknown and also sanctioned the service of defendants by "innovative" methods including Facebook Messenger, Whatsapp and a data room system.

CMOC was the victim of a business email compromise fraud. The perpetrators had hacked into CMOC's system and sent payment instruction emails to its bank, purporting to come from an authorised signatory. In response to those instructions, the bank paid USD6.91 million and EUR1.27 million out of CMOC's account in twenty separate transfers.

The first defendant was a group of persons whose identities were unknown. The second to 31st defendants were named individuals or entities, which CMOC had identified through information and disclosure orders against the banks into which the funds had been paid. These banks, of which there were 50 in 19 different jurisdictions, were "no cause of action defendants". No substantive relief was claimed against them but they were joined to the proceedings as respondents to the information and disclosure orders that were made.

The claims brought against the 31 defendants were: proprietary claims involving the use of tracing; a claim for compensation for dishonest assistance; a claim in damages for unlawful means conspiracy; a claim in knowing receipt; and a claim in unjust enrichment. The court held that all of the claims against all of the relevant defendants succeeded as pleaded (with the exception of the unjust enrichment claim, which succeeded against only some of the defendants).

Obligation of fair presentation in absence of defendants

None of the 31 defendants engaged in the proceedings. The court reiterated that it nevertheless had to be satisfied on the balance of probabilities that the claims were made out, which, where the underlying allegation was fraud, required cogent evidence. The court made clear that although there was an obligation of fair presentation where a trial was not attended by the defendant, that obligation was less extensive than the duty of full and frank disclosure on a without notice application.

CMOC presented evidence on the destination of the funds paid out of its account in the form of a flow chart. It also provided a summary for each defendant, setting out all the details it had managed to obtain, including date and place of birth, passport number, associated addresses, telephone numbers and email addresses, and Facebook and Whatsapp account details. Agreeing with the proposal put forward by CMOC, the court took a "reasonable and proportionate approach" to the evidence and audited some example payments. It concluded that CMOC's chart provided an accurate summary of the payment flows and there was no reason not to take the whole of it at face value.

World-wide freezing orders

In October 2017, the court had granted a world-wide freezing order (**WFO**) against the first defendant, which was the first such order granted against persons unknown. In its latest decision, the court stated that jurisdiction to grant WFOs against persons unknown was now "clearly established". The court highlighted the recognition in cases such as ***PML***[1] ***and Clarkson***[2] that injunctive relief against persons unknown is particularly apposite where the reason they are unknown is because of their activity as hackers.

Service by Facebook Messenger, WhatsApp and data rooms

The methods of service permitted by the court were, in the judge's own words, "innovative features" of this case. In CMOC's summary for each defendant it set out precisely how that defendant had been served at the relevant stages of the proceedings through to trial. The court concluded from these summaries that the decision of the defendants not to participate in the proceedings was voluntary and informed.

The alternative methods of service that were permitted in these proceedings included use of Facebook Messenger and Whatsapp. The court commented that Whatsapp has the "particular virtue" of showing when a message has been sent and when it has been read by the recipient. Having observed the methods used and ultimately permitted in these proceedings, the judge stated that "the court will consider proactively different forms of alternative service where they can be justified in a particular case".

CMOC had also come up with a system for serving the many banks to which funds had been paid with all the evidence adduced in obtaining the interlocutory orders, which the court approved. This system involved sending the relevant party, by way of a previously approved court method (including email), a link to a data room and an access code. Any party which accessed the data room would be able to view all the evidence along with all applications and orders made as at that date. The court commented that the banks had found the data room "a most useful facility". As with Facebook Messenger and Whatsapp, the court observed that service by data room could clearly be justified and appropriate in cases such as this.

COMMENT

This case confirms the English court's willingness to adopt innovative approaches proposed by claimants who are seeking relief from defendants who have concealed their identities. The decision will be welcomed by companies who are faced with the constant threat of cyber attacks by anonymous hackers. As the court recognised in this case, in cases of international fraud a freezing injunction is often needed as a "springboard for the grant of ancillary relief". The court also recognised that vital information is likely to be obtained from banks as to the identity of account holders, which may result in the claimant being able to subsequently name them as defendants, as happened here.

Even where the defendant is not unknown, the English High Court has recently shown its ability to assist the innocent party in a cyber dispute by allowing it to bring a claim against a defendant domiciled in another jurisdiction. In *BVC v EWF*,[3] the court held that it was able to hear a claim for damages for misuse of private information, despite the fact that the defendant said he was domiciled in Switzerland, on the basis that England was where the claimant had his "centre of interests". Following the CJEU in *eDate Advertising*,[4] the court found this basis for jurisdiction to be appropriate in the context of online publication of information, where distribution was essentially universal. In addition, service by email was deemed effective even though the defendant was in Switzerland when he received the email.

Prospective claimants should be encouraged by the court's flexibility in these cases and its willingness to embrace mechanisms in order to allow victims of cyber crime to pursue effective legal remedies.

Elizabeth Staves
Senior Associate
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 4308
elizabeth.staves@allenovery.com

[1] *PML v Person(s) Unknown* [2018] EWHC 838 (QB).

[2] *Clarkson Plc v Person or Persons Unknown* [2018] EWHC 417 (QB).

[3] [2018] EWHC 2674 (QB).

[4] *eDate Advertising GmbH v X (Cases C-509/09 and C-161/10)* [2012] QB 654.

BANK ORDERED TO DISCLOSE SUSPICIOUS ACTIVITY REPORTS TO CUSTOMER

Lonsdale v National Westminster Bank [2018] EWHC 1843 (QB), 18 July 2018[1]

A bank was ordered to disclose, to a customer, Suspicious Activity Reports (**SARs**) that the bank had sent to the National Crime Agency (**NCA**) at the time of freezing the customer's bank accounts. The bank's arguments concerning confidentiality, tipping-off and prejudicing an investigation were unsuccessful. The court's observations on the interplay between the SARs regime and the law on data protection, defamation and breach of contract will be of interest to all banks.

Suspicious Activity Reports (SARs) – a reminder

A bank may protect itself from committing a money laundering offence under the Proceeds of Crime Act 2002 by making a SAR to the National Crime Agency and obtaining appropriate consent. When a SAR has been submitted a bank will freeze the suspicious accounts. If it has not received a "notice of refusal" from the NCA within seven working days it may unfreeze the account. The level of suspicion required to attach criminal liability to a bank for money laundering is low – and, in part, is a subjective test. Banks are responsible for 82.85% of SARs submitted to the NCA.[2]

Bank submits SARs and freezes accounts

In March 2017 the bank froze a joint account belonging to one of its customers, a barrister, for eight days and in December it froze seven other accounts of the same customer – a personal account, another joint account and four accounts for businesses in which he was a director. The customer requested access to documents relating to the freezing of his accounts. The bank provided limited documentary evidence, and did not disclose the SARs.

Customer does not believe bank held genuine suspicion

The customer launched a multi-pronged attack on the bank's actions, including making claims for breach of contract, defamation, breach of the Data Protection Act 1998 (the acts took place pre-GDPR) and also an application for disclosure of the SARs.

Implicit in all these claims was the customer's beliefs that: (i) the bank did not hold a genuine suspicion that the money in his accounts was the proceeds of crime; (ii) his accounts had been unnecessarily suspended: and (iii) his reputation had been damaged.

The customer wanted to see the SARs and information held by the bank relevant to its decision to make the SARs and freeze (and unfreeze) his accounts. He sought summary judgment on his claims (summarised below).

[1] Only recently made public.

[2] https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/07/Anti-Money-Laundering-the-SARS-Regime-Consultation-paper.pdf

Customer's claims	**Bank's defence/application**	**Court's ruling**
Breach of contract: the bank was in breach of contract by failing to follow the accountholder's instructions and by failing to evidence that it had a genuine suspicion that the account held criminal proceeds.	Express contractual provisions allowed the bank to freeze accounts if not to do so would expose it to criminal liability.	Not a matter for summary judgment since it involved questions of fact – the bank must show that it held the relevant suspicion.
Breach of DPA 1998: the bank: (i) had not provided in time (or at all) all personal data in response to the data subject access request; and (ii) the data provided was not in intelligible form and it included inaccurate information.	The decision to freeze accounts did not concern "personal data". The information sought contained that of other individuals (so it was mixed data) and there was an exemption for the prevention and detection of crime.	The customer's claim was not a matter for summary judgment. However, the bank's approach to determining whether information was the customer's personal data was "clearly flawed" and the customer had a "strong claim" that the bank's deliberations and decision to submit SARs and freeze and unfreeze accounts was based on his personal data. Accordingly the banks application for strike out/summary dismissal was rejected.
Defamation: the bank had defamed the customer by suggesting that it had suspicions that his account contained criminal proceeds. Defamatory statements were published in the SARs and in internal bank employee communications concerning the decision to make the SARs and freeze the accounts.	The statements were not defamatory, not published, did not cause harm and in any case were protected by qualified privilege.	Not a matter for summary judgment: statements were capable of being defamatory and they were published. However qualified privilege was likely to apply, subject to malice.

Customer's claims	Bank's defence/application	Court's ruling
Inspection: The customer was entitled to see the SARs as they had been referred to in the bank's defence and counterclaim.	SARs are, in general, confidential, and these SARs were disclosed to NCA in the strictest confidence. Permitting inspection of the SARs may expose the bank to the offence of tipping-off or prejudicing an investigation. Inspection was not necessary for fair disposal of action.	The SARs in question must be disclosed after 14 days of the court's order (to enable NCA to consider its position on making such disclosure). There was no evidence that inspection would trigger tipping-off. There was no evidence that they are required to be kept confidential. The SARs were plainly relevant to the assessment of whether the bank's employees genuinely held a relevant suspicion.

Impact of decision

This was a summary judgment/strike out application, so is of limited precedent value. The case has settled so we will not see the issues that arose fully resolved.

We are not expecting this decision to cause a rush by customers to bring claims of this sort against banks:

- Courts have historically provided banks with considerable protection and discretion relating to SARs due to the fact that banks are merely seeking to help law enforcement and avoid criminal liability. The courts would not want to encourage civil claims of this sort.
- It is hard to imagine why a bank would file a SAR without a genuinely-held suspicion (even if that suspicion turns out to unfounded).
- Many customers would be deterred by the potential cost. The claimant in this case was a barrister who represented himself so this aspect was less of an issue for him.

The ruling does however provide a reminder that should a bank be faced with a similar claim, it is very unlikely to be able easily and quickly to defeat it (by way of strike out). The ruling makes clear that the question of whether a bank has a genuine suspicion that money in an account was criminal property is a primary fact for the bank to prove at trial.[3]

Banks may start receiving data subject access requests for personal data relating to SARs. The judge's view on this summary judgment application was that there was a "strong case" that a bank's deliberations and decision to submit SARs and freeze accounts constituted personal data, and that the bank had demonstrated "a flawed understanding of the scope of that concept". Since it was a summary judgment application, the judge felt unable to address whether the exemption relating to the prevention or detection of crime was available stating "[t]here is no evidence before me regarding the likelihood of the provision of further personal data to Mr Lonsdale prejudicing the prevention and detection of crime." It is difficult to imagine that the rules relating to tipping-off would not prevail since it seems to be a paradigm example of what the crime exemption was aimed at (provided the bank held a genuine suspicion). It is a shame that the judge did not feel able to make this finding even on a summary basis.

Looking ahead

There is a call for reform of the UK's SARs regime. The OECD has criticised the UK for the low level of corruption enforcement activity from the current regime. A UK Law Commission consultation states that there are on average 2000 SARs filed per day with the NCA, many of 'low quality', making it hard for investigation authorities to detect where the real risks are.

The low level test for suspicion for the substantive money laundering offences in the UK has also been criticised in the consultation. "A majority of

stakeholders expressed the view that suspicion remains ill-defined, unclear and inconsistently applied by banks and businesses." This leads to defensive reporting where reports are made more because of concerns regarding a failure to comply with POCA than because of genuine suspicion.

The Law Commission recommends improvements to the SARs regime, in particular suggesting that better guidance on 'suspicion' would lead to better quality SARs.

If you would like to discuss the issues arising from this case, including how to respond to data subject access requests in the SARs context, please contact Arnondo Chakrabarti, Eve Giles or your normal Allen & Overy contact.

Arnondo Chakrabarti
Partner
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 4424
arnondo.chakrabarti@allenovery.com

Eve Giles
Partner
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 4332
eve.giles@allenovery.com

Amy Edwards
Senior Professional Support Lawyer
Litigation

Contact
Tel +44 20 3088 2243
amy.edwards@allenovery.com

Jason Rix
Senior Professional Support Lawyer
Litigation

Contact
Tel +44 20 3088 4957
jason.rix@allenovery.com

3. Applying *Shah v HSBC Private Bank* [2009] EWHC 79 (QB).

Data Protection

EMPLOYER VICARIOUSLY LIABLE FOR ROGUE EMPLOYEE'S DATA BREACH

WM Morrison Supermarkets PLC v Various Claimants [2018] EWCA Civ 2339, 22 October 2018

An employer was held by the Court of Appeal to be vicariously liable for a rogue employee's deliberate and criminal disclosure of the personal data of other employees. This was despite the employee's aim being to harm the employer – rather than for any personal gain or to injure third parties – and the fact that the employer had not itself breached data protection legislation. The retailer has said it will seek permission to appeal to the Supreme Court.

This group litigation followed the intentional disclosure by a disgruntled rogue employee, Mr Skelton, of the personal details of nearly 100,000 employees. As part of his job, Skelton had been given access to payroll data in order to provide it to the employer's auditors. However, he copied that data, whilst at work, onto a personal USB stick and posted it onto a file-sharing website. Skelton was convicted and charged with fraud and offences under the Data Protection Act 1998 (**DPA**) and the Computer Misuse Act 1990. Around 5500 employees brought this claim for damages for the misuse of private information, breach of confidence and breach of statutory duty under the DPA.

This appeal related only to vicarious liability. The first instance finding that Morrisons bore no primary liability stands.

Although the case was decided under the DPA, the principles are equally applicable under the Data Protection Act 2018 and the GDPR.

DPA does not exclude vicarious liability

The employer had to show that the DPA excluded vicarious liability for breach of statutory duty under the DPA and at common law (for misuse of private information and breach of confidence). It argued that the DPA is a comprehensive code for data breaches of this kind and so excludes any vicarious liability for the wrongful processing of data by an employee. The court disagreed holding that vicarious liability is not confined to common law wrongs: it applies equally to breaches of statutory duty, provided the statute does not state otherwise because:

- If Parliament had intended such a "substantial eradication" of common law rights, it would have expressly stated so.
- Although the argument was all about vicarious liability, the employer had to accept that primary liability for the misuse of private information and breach of confidentiality is not excluded by the DPA. The court viewed this as inconsistent with one of the main objects of the DPA (the protection of privacy and the provision of an effective remedy).
- The DPA does not overlap with common law; it is only concerned with the primary liability of the data controller (whom both parties accepted was Skelton and not the employer) and there are no provisions in the DPA addressing the situation of an employer whose employee data controller breaches it.

Test for vicarious liability satisfied

Having decided that the DPA did not exclude vicarious liability, the court applied a two-stage test to decide whether the employer was vicariously liable. The test is based on the Supreme Court's decision in *Mohamud v WM Morrison Supermarkets plc* [2016] UKSC 11.

Stage 1: ascertaining the 'field of activities' of the employee

The employer had entrusted Skelton with its payroll data: his role was to receive it, store it and to disclose it to a third party (the auditor). The court determined that the fact he chose to disclose it to other (unauthorised) third parties was "*nonetheless closely related to what he was tasked to do*".

Stage 2: whether there is a sufficient connection between the employee's field of activity and the wrongful conduct

Sufficient connection is usually found where the employee uses or misuses the position entrusted to him thereby injuring a third party; the court concluded that since the employer selected the employee it is right under principles of social justice that the employer should be responsible.

The employer argued that there was insufficient connection because the unlawful disclosure by Skelton had been done at home, on his own computer, outside of working hours, and several weeks after he had originally downloaded the data. The court disagreed holding that:

- The claimants' cause of action was already established when Skelton was at work when he improperly *downloaded* the data, rather than when he subsequently disclosed it online.
- Vicarious liability does not only apply if the employee is "on the job"; although the time and place when the relevant act occurred are relevant, they are not conclusive. The court referred to numerous cases in which employers had been vicariously liable for torts committed away from the workplace, including *Bellman v Northampton Recruitment Ltd* [2018] EWCA Civ 2214 (discussed below).
- It approved the trial judge's findings on sufficient connection:
  - an unbroken thread linked Skelton's employment to the disclosure as a "seamless and continuous sequence of events";

- the employer intentionally entrusted Skelton with the data during the course of his employment; and
- the employer tasked Skelton with receiving, storing and disclosing the data; therefore his actions (albeit unlawful) were closely related to the task he was given.

Employee's motive irrelevant

Since Skelton's intention was to harm Morrisons, rather than benefit himself or injure a third party, the retailer argued that, if it were found vicariously liable, this would render the court an accessory in furthering Skelton's criminal aims. The court disagreed holding that the employee's motive is irrelevant and an intention to cause financial or reputational harm to the employer was no exception and could not prevent a finding of vicarious liability.

Vicarious liability for torts committed away from the workplace

A differently constituted Court of Appeal handed down its judgment in *Bellman* just under a fortnight before the appeal in this case. In *Bellman*, the defendant company, Northampton Recruitment, was held to be vicariously liable for an assault committed by its managing director, Mr Major, on another employee after a work Christmas party. Mr Major was held to be still acting as Managing Director at a separate drinking session, which took place after the Christmas party and was where the assault occurred, rather than as a "mere reveller". The judgment, whilst recognising that the facts giving rise to vicarious liability were unusual, provides a useful analysis as to how vicarious liability can play out away from the workplace.

Implications for employers

The starkness of this case for employers is that Morrisons was not primarily liable under the DPA and the Information Commissioner's Office (**ICO**) had decided that no enforcement action against Morrisons was necessary. Nonetheless it was still held to be vicariously liable for the actions of an employee acting out of malice.

The court was not swayed by the impact of placing this burden on an 'innocent' employer; it was more concerned that victims would otherwise be left with no remedy except against the individual employee, adding that the solution is for employers to insure against such losses. However, the likely premium for this type of insurance cover may well make it prohibitively expensive, especially when customer data is taken into account.

As noted above, this case was decided under the DPA. However, the principles of vicarious liability would be the same in respect of the Data Protection Act 2018 and the GDPR. Indeed, it is possible we may see more group litigation claims due to increased data subject awareness and the fact the GDPR actively encourages group claims for data breaches.

Morrisons are seeking leave to appeal to the Supreme Court.

Hugo Flaux
Associate
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 2675
hugo.flaux@allenovery.com

Jason Rix
Senior Professional Support Lawyer
Litigation

Contact
Tel +44 20 3088 4957
jason.rix @allenovery.com

Nathalie Burn
Legal Practitioner – Returnship Programme
Litigation

Contact
Tel +44 20 3088 1316
nathalie.burn@allenovery.com

Equity

SECURED CREDITOR HAS EQUITABLE DUTY TO PERFECT, BUT NOT NECESSARILY TO PROTECT, SECURITY FOR BENEFIT OF A GUARANTOR

General Mediterranean Holding SA.SPF (aka General Mediterranean Holding SA) v Qucomhaps Holdings Ltd, William James Harkin (& anr) [2018] EWCA Civ 2416, 31 October 2018

Although a secured creditor has an equitable duty to perfect its security, there is no "absolute" duty on a creditor to preserve or maintain the security for the benefit of a guarantor. A creditor may however be required to take non-onerous steps to preserve or maintain third party security for the benefit of a guarantor. There was also no implied contractual duty on the creditor to take further steps to protect the security. The borrower and guarantor were liable to repay the loan, despite the fact that the third party security for the loan had been distributed to alleged fraudsters in a Czech insolvency rather than preserved for the secured creditor. The dispute reinforces the importance of market standard clauses aimed at avoiding arguments as to what steps a secured creditor must take to protect its security.

The claimant creditor (the **Creditor**) had made loans (the **Loans**) to Qucomhaps (the **Debtor**) to finance the purchase of the assets of a Czech aircraft manufacturing company. Although the original advances were not documented in any binding loan agreement, agreements were later signed under English law to document the loan and provide a guarantee by Mr Harkin (the **Guarantor**). As part of the security arrangements, a wholly-owned subsidiary of the Debtor, Morovan, provided third party security (the **Security**) by way of a charge over its assets. Moravan subsequently went into administration in the Czech Republic. The Creditor declined to file a secured creditor's claim in the Czech administration and the Security was lost to other, allegedly fraudulent, purported creditors of Moravan.

The Creditor brought proceedings to recover the sums due under the Loans against the Debtor and the Guarantor (together, the **defendants**). The defendants argued that, as the Creditor had failed to take steps necessary to protect the Security, neither party was liable. That defence was struck out and the Creditor obtained summary judgment. This was upheld on appeal to the High Court when it refused to imply terms in the loan and guarantee agreements to the effect that the Creditor was under a duty to take the required steps in the Czech proceedings to preserve its rights in respect of the Security. The defendants obtained permission for a second appeal to the Court of Appeal on the ground that the case raised an important point of principle concerning the extent of a secured creditor's equitable duty to a guarantor – which had been dealt with only briefly by the High Court. The Court of Appeal considered only the question of whether the Creditor had breached its equitable duties to both the debtor and guarantor by failing to take reasonable steps to protect the Security.

Creditor does not have a general duty to guarantor to protect the security

The court rejected the defendants' argument that a creditor has a broad equitable duty to the guarantor to take "reasonable steps to protect" its security. The court considered the scope of a secured creditor's duty to a guarantor.

Duty owed to guarantor to perfect security – although a flexible concept

The court considered that it was clear law that where a secured creditor also has the benefit of a guarantee, it has an equitable obligation to perfect the security and thereafter not to release or surrender it. If the creditor neglects these duties it will lose the benefit of the

guarantee (to the extent that it could have been satisfied by the security).

Counsel for the Creditor submitted that a lender has no other duty to take positive steps to preserve the security unless expressly agreed with the guarantor or debtor (although, of course, where a creditor chooses to enforce security (such as exercising a power of sale) it also has a duty to take reasonable steps to obtain a proper sale price). However, the court was doubtful that this was as far as the duties on a creditor go – unless perhaps the notion of "perfecting" the security was treated flexibly. Newey LJ considered for example that, if to maintain the validity of the security the creditor was required not only to register it but also to pay a "modest" annual fee, then there would be a "strong case" for saying that the creditor would have a duty to pay that fee.

No absolute or onerous equitable duty to guarantor to preserve or maintain security

On the other hand, the court was keen to stress that any duty to "preserve or maintain" security is not an onerous one. A creditor has no "absolute" duty to ensure a guarantor has recourse to the security. A creditor is not obliged to "incur any sizeable expenditure or run any significant risk" to preserve or maintain a security. There is no duty to preserve or maintain the security "at the peril of the creditor".

One of the reasons given by the Creditor as to why it did not claim in the Czech insolvency proceedings was that it understood that the Security might be unenforceable in the Czech courts and that, had its claim failed, it could have been ordered to pay compensation equal to the amount of the claim. The court agreed that the Creditor was not under any obligation to expose itself to such a risk.

The court was receptive to the Creditor's arguments that recognising a wider duty to protect security would be commercially impractical as it would:

- introduce undesirable uncertainty;
- be detrimental to the ability of a lender to carry on business; and
- be anomalous in circumstances where the law does not require a creditor to do anything to prevent the security losing its value (as opposed to preserving its availability to the creditor or guarantor).

Ultimately any hardship to a guarantor is resolved by the guarantor's right to pay off the loan and take control of the security itself.

No duty owed to the debtor in relation to third party security

The court was rather more robust in relation to any duty to a debtor. It was doubtful that a creditor could ever owe any equitable duty to a debtor to take steps to preserve or maintain a security granted by a third party. This would not make sense in circumstances where that security was never something to which the debtor would have recourse

No implied terms to protect security

This aspect of the High Court's decision was not appealed. By way of reminder, Sir David Eady (sitting as a Judge of the High Court) stated that the court will be reluctant to imply a duty that a creditor must take the necessary steps to preserve its security rights into a contract where no duty exists in law or in equity. The defendants argued that it was appropriate to imply such a term in this instance as the Creditor would have known that the defendants could only repay the Loans using the Security. The court disagreed as the ability to repay a loan usually depends on a range of factors. In any case it did not necessarily follow that even if the Creditor had known this it would have given rise to the contended duty.

The High Court concluded that there was no chance of implying the terms proposed as they were not necessary to give business efficacy and, far from being the "obvious" intention of the parties, the situation was one which almost certainly would not have crossed the parties' minds. There was no realistic prospect, therefore, that the Creditor was under a duty to take a particular step in foreign court proceedings merely because it would or may have preserved the Security.

COMMENT

The result of this litigation is unsurprising but will provide comfort to lenders that they do not owe duties to

debtors and guarantors, absent express agreement, to take onerous steps to enforce or protect their security. This is consistent with the principle established by the Privy Council in *China & South Sea Bank v Tan Soon Gin* that a creditor is not obliged to exercise its powers in relation to its security in any particular way.

However, the suggestion that a creditor's duties may go beyond merely "perfecting" and extend to "preserving or maintaining" the security, albeit on a qualified basis, does introduce some uncertainty. When would a step become too "significant" a risk or too "sizeable" an expenditure such that the creditor cannot be expected to take it? In market standard documentation there are important clauses which guard against such uncertainty. Parties typically agree that:

- any failure by a creditor to exercise a right or remedy under a loan document does not act as a waiver of that right;
- guarantors or providers of third party security explicitly waive any defence arising from the failure of a creditor to perfect or enforce security over any secured assets; and
- debtors waive any right, subject to certain exceptions, that they have to require that the security be enforced in any particular order or manner or at any particular time.

This is a sensible position that leaves it up to a creditor's commercial judgement as to how to deal with its security.

Jon Turnbull
Associate
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 3326
jon.turnbull@allenovery.com

Nathalie Burn
Legal Practitioner – Returnship Programme
Litigation

Contact
Tel +44 20 3088 1316
nathalie.burn@allenovery.com

Privilege

IN-HOUSE COUNSEL EMAILS NOT PRIVILEGED

Glaxo Wellcome UK Ltd (t/a Allen & Hanburys) & anr v Sandoz Ltd & ors [2018] EWHC 2747 (Ch), 25 October 2018

Emails between an in-house counsel and an employee, gathering information to provide to external lawyers, were **not** protected by legal advice privilege. The decision illustrates (a) how difficult it will be for internal fact finding to be privileged in the absence of existing or contemplated litigation, and (b) the importance of establishing, for communications between in-house counsel and an employee, whether legal advice privilege applies.

In the context of an intellectual property dispute, the defendants, who were all in the same group of companies, had to disclose documents relating to the design history of a product. They claimed privilege over emails between an in-house lawyer and a regulatory affairs manager, who both worked at one of the defendant group companies.

These emails either sought, or provided, information to give to external lawyers. The claimants challenged the defendants' claims to privilege over these emails.

Regulatory affairs manager not authorised to seek legal advice from external legal advisers

The defendants claimed that the regulatory affairs manager was authorised to request and receive legal advice where it was relevant to his regulatory affairs position, and that it was within the scope of his authority to provide information for the purposes of obtaining legal advice. Communications between him and the in-house counsel were, the defendants argued, therefore privileged.

The court found that there was no evidence that the regulatory affairs manager was authorised to seek legal advice from the external lawyers, who were in fact acting for another group company. It was more likely, the court said, that the in-house counsel had been tasked with that job and it was the in-house counsel that was obtaining information for that purpose. In that event, the court held, the in-house lawyer's exercise in gathering information from the regulatory affairs manager would not be subject to legal advice privilege: "The provision of information by him [the regulatory affairs manager] would not make the communication privileged unless he was the client for the purposes of him obtaining legal advice" (which he was not).

Group companies had not each made out their claim to privilege

The defendants' evidence in support of their claim to privilege did not explain each of their respective entitlements to privilege. The court criticised this approach. The court noted that there was no evidence that the external law firm in question was providing advice to the company for which the in-house counsel and regulatory affairs manager worked, nor that the regulatory affairs manager had any authority to seek legal advice from that external law firm (who was acting for another group company).

The court concluded that the emails were not privileged.

Comment

This decision confirms that the gathering of information by in-house counsel of a company, from an employee of that company, for passing on to external lawyers in order for advice to be provided by that external law firm is not privileged.

Who is the "client"?

This decision makes it clear that, as Andrews J said in *SFO v ENRC*:[1] "…the employee must be authorised to seek/obtain the legal advice that is the reason for the communication…". So, while an employee may well be authorised to obtain legal advice from in-house counsel, s/he may not be so authorised in relation to an external law firm. The question of who is the client in respect of any given communication is a question of fact.

The decision further reiterates that the mere fact that an employee is generally authorised to communicate with or give information to a lawyer is not enough to make that employee the "client" *vis-à-vis* that lawyer. This is consistent with *RBS Rights Issue Litigation*:[2] "the fact that an employee may be authorised to communicate with the corporation's lawyer does not constitute that employee the client or a recognised emanation of the client".[3]

It is worth remembering that just because someone holds the office of in-house counsel does not mean that s/he is automatically a "client" of external legal advisers for privilege purposes. As Andrews J put it in *ENRC*: "It might also be persuasively argued that the company's in-house lawyers or general counsel would have the necessary authority, by virtue of their office, to seek and obtain legal advice from external lawyers on behalf of the company. Whether they, or any other individual employee or group of employees had such authority in a given case, is a question of fact to be determined on the evidence."[4]

Accordingly, companies may need to look at employee job descriptions to assess whether individuals are authorised to seek and obtain legal advice and, if so, who from. The answer is not always clear-cut.

Group companies must be specific when claiming privilege

The decision highlights the importance of being aware, when undertaking a privilege analysis, of the lines of communication both within a company and between companies in the same group, particularly where there

may be some shared legal function. Any evidence put forward in support of a claim for privilege on behalf of a number of group companies must explain clearly each company's entitlement to the privilege and, although not relevant here, where advice is being given by an in-house lawyer in one company to an employee in another company, it is important to assess carefully whether this might impact the question of whether the employee can be said to be a client for privilege purposes.

Internal and external legal advice

It seems that there was no suggestion in this case that, in relation to the emails in question, the in-house counsel had intended to, or provided legal advice to the employee – the defendants stated that she was simply seeking information to pass on to external lawyers. So there does not seem to have been a basis for arguing that the emails were privileged communications between the employee (as client) and the in-house counsel (as lawyer). However, on the right facts it may of course be possible to make such a claim to privilege. For example, an in-house counsel may initially request and receive information in emails with an employee with the intention of subsequently providing legal advice to that employee. In-house counsel may decide to pass on the same information to an external lawyer, perhaps for a second opinion or a more detailed analysis, or in connection with a separate matter. This latter action does not affect the privilege analysis of the original emails.

The purpose for which an information gathering exercise originally took place (was it to simply pass on to external lawyers as in this case, or was it for the in-house counsel to advise his/her "client"?) may not always be documented in the context of busy day-to-day corporate operations. Where litigation privilege is not available, in-house counsel should ensure they consider carefully who their internal clients are on any given matter and, even when they are communicating with an employee who would ordinarily fall within that "client" category, they must consider whether that particular communication involves the lawyer wearing his/her "lawyer" hat and the employee wearing his/her "client" hat or whether the communication is in fact made on some other basis. If it is unclear whether an individual is a client for these purposes or whether either party is wearing the right hat in relation to a particular communication, it may be prudent to operate on the basis that the communication will not be privileged.

Amy Edwards
Senior Professional Support Lawyer
Litigation

Contact
Tel +44 20 3088 2243
amy.edwards@allenovery.com

[1] The court noted that this quote was cited with 'apparent approval' by the Court of Appeal in *ENRC v SFO*.

[2] See Investigations: notes of employee interviews not privileged.

[3] Hildyard J in *Re RBS Rights Issue Litigation*.

[4] Para 92 Andrews J *SFO v ENRC*.

Public law

DECISIONS OF A PRIVATE BODY ACTING AS A "SKILLED PERSON" CANNOT BE JUDICIALLY REVIEWED

R (Holmcroft Properties Ltd) v KPMG LLP & ors [2018] EWCA Civ 2093, 28 September 2018

In an important decision on when private bodies can be subject to judicial review, the Court of Appeal confirmed that KPMG's decisions as a "Skilled Person" (per s166 Financial Services and Markets Act 2000 (FSMA)) in a bank's voluntary redress scheme for customers mis-sold interest rate hedging products could not be reviewed by the court. Conducting a detailed analysis of the authorities in this complex area of public law, the Court of Appeal found that KPMG was not exercising a public function which was amendable to judicial review; the nature of the redress scheme was essentially for the pursuit of private rights in a private law context.

KPMG appointed as "skilled person" in redress scheme

Following the (then) Financial Service Authority's (**FSA**) investigation into various banks' sale of interest rate hedging products to customers, Barclays Bank plc voluntarily agreed to provide compensation to affected customers. As part of that arrangement, the bank agreed to appoint a "skilled person" under s166 FSMA, and subsequently engaged KPMG LLP to perform that role.

The skilled person had to be approved by the FSA, would report to the FSA on the operation of the redress scheme and would provide an opinion to the bank as "Independent Reviewer" on whether each offer of redress made to a customer was appropriate, fair and reasonable – such an offer would only be made if the Independent Reviewer confirmed it was appropriate.

The appeal centred on whether KPMG's decisions as Independent Reviewer were subject to judicial review. The appellant, a customer dissatisfied with the compensation offer made by the bank and approved by KPMG, argued that KPMG's decisions could be judicially reviewed and claimed that KPMG's approval of its offer was unfair. KPMG, the bank and the (now) FCA all argued that judicial review was not available and that in any event there was no public law breach.

When decisions of private bodies are subject to judicial review

Under English public law, entities other than public bodies can be subject to judicial review in certain limited circumstances, meaning that a third party with a sufficient interest in a matter can bring a challenge against the decision in question in the Administrative Court. This is because amenability to judicial review depends on whether the body is exercising functions of a public law nature, and non-public bodies can in some circumstances exercise public functions – it is the nature of the particular act or decision that is key, rather than the body's formal status.

There is no strict test for when a non-governmental body will be subject to judicial review and it is a fact-sensitive question. The courts have found judicial review to be appropriate where, for example, the government would assume control of the function if the body in question was not doing it, or where the body is "woven into the fabric of public regulation or into a system of governmental control". No single factor is determinative and the court will take into account whether there is governmental or statutory underpinning for the function, the substance and effect of the function being discharged, the public importance of the function being performed, and the source of the powers being exercised.

At first instance, the court took particular note of the fact that the redress scheme was voluntary, KPMG's functions were conferred by contract and KPMG was not appointed by the FSA itself (although the FSA had to confirm the appointment). It therefore concluded that the role of Independent Reviewer did not have a sufficient "public law flavour" to make KPMG amenable to judicial review. Although it came to the same conclusion, the Court of Appeal took a wider approach to the assessment of whether KPMG was exercising a public function than the court below.

Not too much focus on source of powers

The Court of Appeal considered that the Administrative Court had put too much focus on the source of KPMG's powers.

The Court of Appeal did not consider the fact that the arrangements underpinning KPMG's role were contractual to be decisive. It took a broader approach to the question of whether KPMG was carrying out a public function, looking at all relevant circumstances including the regulatory context and the independent reviewer's function within the scheme. Considering the regulatory context, the fact that the bank voluntarily accepted the redress scheme did not necessarily mean that the entities involved were not exercising functions of a public law nature – that would reflect too narrow a view of the FSA's statutory functions and aims. However, the Court of Appeal did think it was particularly relevant that the FSA was not involved in negotiations with individual customers and therefore did not have a hands-on role in the operation of the scheme.

Redress scheme was for pursuit of private law rights

The Court of Appeal held that the nature of the scheme was for the pursuit of private rights – it was ultimately a mechanism for providing compensation arising from the bank/customer private law relationship, and the compensation covered was to be negotiated and could be challenged on private law principles. If judicial review was not available, customers would not be left without a remedy: if they did not like KPMG's determination, they could reject it and pursue a private law claim. To put the matter beyond doubt, the Court of Appeal also considered whether there would have been any public law breach, had it decided that KPMG could be subject to judicial review. The court unanimously confirmed that there were no grounds for complaint and that it would have dismissed the claim.

COMMENT

Private bodies – and particularly those acting as a skilled person or carrying out another role in a regulatory context – have welcomed this decision. Although it will always be fact sensitive, the judgment offers helpful guidance on the factors that the court will consider when determining amenability to judicial review.

From a consumer perspective, the court acknowledged that it exposed a gap in protection where an affected customer did not know that it should exercise its private law rights to challenge an offer. For example, while a customer could decline an offer and pursue a misselling claim instead, that did not help customers unaware of any defects. Nonetheless, the court noted that the redress scheme did not guarantee that every customer would receive an appropriate offer. As the court did not consider that this vacuum was its to fill, it remains to be seen if the FCA will change its approach in devising future redress schemes.

Maeve Hanna
Senior Associate
Litigation – Litigation & Investigations

Contact
Tel +44 20 3088 1844
maeve.hanna@allenovery.com

Sanctions

MERE RISK OF EXPOSURE TO SANCTIONS INSUFFICIENT FOR UNDERWRITERS TO AVOID LIABILITY

Mamancochet Mining Ltd v Defendants Managing Agency Ltd [2018] EWHC 2643 (Comm), 12 October 2018

Underwriters could not rely on a sanction limitation and exclusion clause in an insurance policy, which referred to insurers' "exposure" to sanctions, to avoid liability for a claim simply because there was a risk that the Office of Foreign Assets Control (OFAC), the U.S. sanctions regulator, might conclude the payment was prohibited and potentially impose a sanction. "Exposure" to sanctions means that any payment under the claim must be prohibited by law. The case also provides *obiter* comments on the clash between recently re-imposed U.S. sanctions in relation to Iran and the EU "Blocking" Regulation.

The defendant underwriters of a marine insurance policy (the **Policy**) alleged that they were not liable for a claim made for theft of a shipment of goods whilst the vessels were in Iran, intended for an Iranian national. They relied on a sanctions clause in the Policy (the **Sanctions Clause**) that they should not have to pay any claim if it would "expose" them to various sanctions, including those made under U.S. and EU law.

U.S. sanctions

The U.S. sanctions, on which the defendants relied, are the recently re-imposed Iranian Transactions & Sanctions Regulations (the **U.S. Sanctions**), following the U.S.'s departure from the agreement of the Joint Comprehensive Plan of Action to grant Iran relief from various international sanctions in May this year. The prohibitions include the provision of insurance cover and payment of a pre-existing claim where there is an Iranian connection. Although the defendants were UK-based, the U.S. Sanctions were relevant as a number of them were "U.S. owned or controlled foreign entities".

"Exposed" to a sanction means conduct is currently prohibited in law

The High Court construed the Sanctions Clause as meaning that the insurers must show that payment is in fact prohibited by law – at which point OFAC may or may not penalise the prohibited conduct with a sanction. Simply being exposed to the risk of being sanctioned, as suggested by the defendants, was insufficient. The court concluded that the U.S. Sanctions did not, in fact, prohibit payment of the insurance claim, because the relevant sanctions were not coming into force until 11.59pm EST on 4 November and therefore payment before then would not "expose" the defendants to the U.S. Sanctions. They were therefore liable to pay out under the Policy. It was common ground that payment after that time would be prohibited.

EU "Blocking" Regulation not engaged

The court also considered the EU "Blocking" Regulation, which aims to protect against the extra-territorial application of certain legislation adopted by a third country (the **Blocking Regulation**). This has been recently updated to expressly prohibit EU persons from complying with the U.S. Sanctions against Iran. The combined effect of the Blocking Regulation and the U.S. Sanctions means that the respective laws now directly conflict, leaving businesses with a difficult decision (see: Iran Sanctions and the EU Blocking Regulation: navigating legal conflict). Some judicial observations on this conflict, albeit *obiter*, were made by the court.

Although the payment was not, in fact, prohibited by the U.S. Sanctions (meaning that there was in fact no conflict with the Blocking Regulation), the court considered whether the Blocking Regulation would have prevented the defendants from relying on the Sanctions Clause. Although it did not reach a definitive view, it saw considerable force in the argument that the Blocking Regulation is not engaged if an insurer's liability is suspended under a sanctions clause. This is because an insurer is not "complying" with a third country's prohibition, but simply relying on the terms of a policy to resist payment.

COMMENT

The Sanctions Clause was based on standard industry wording. Insurers will now need to review their sanctions wording. The court suggested that had the wording been along the lines of "exposure to the risk of being sanctioned" or "conduct which the relevant authority might consider to be prohibited", it would have agreed with the defendants' interpretation of the Sanctions Clause.

The decision is interesting as it provides the first insight into the approach of the English court to the interplay between the U.S. sanctions against Iran and the EU Blocking Regulation, although note the comments were *obiter* and at first instance.

Jason Rix
Senior Professional Support Lawyer
Litigation

Contact
Tel +44 20 3088 4957
jason.rix @allenovery.com

Nathalie Burn
Legal Practitioner – Returnship Programme
Litigation

Contact
Tel +44 20 3088 1316
nathalie.burn@allenovery.com

Sovereign immunity

ASSETS OWNED BY A STATE-OWNED ENTERPRISE NOT IMMUNE FROM ENFORCEMENT

Botas Petroleum Pipeline Corporation v Tepe Insaat Sanayii AS [2018] UKPC 31, 22 October 2018

Assets owned by a state-owned entity (SOE) are not "property of a State" and therefore not immune from enforcement under the State Immunity Act 1978 (SIA). This case has important implications for commercial parties contracting with SOEs.

Tepe Insaat Sanayii AS (**Tepe**), a Turkish construction company, and Boru Hatlari Ile Petrol Tasima AS (**Botas**), a Turkish state-owned enterprise, entered into two construction contracts. Following Botas' termination of those contracts, Tepe successfully brought arbitration proceedings against it, obtaining two ICC awards worth approximately USD100 million (the **Awards**). Tepe subsequently sought to enforce the Awards against shares held by Botas in two Jersey subsidiaries (the **Shares**) (The SIA extends to Jersey, with minor modifications). It was common ground that Botas was a 'separate entity' within the meaning of s14 SIA and therefore unable to claim state immunity itself.

The Privy Council rejected Botas' appeal against the decision of the Court of Appeal of Jersey, which had held that Tepe was entitled to enforce the Awards

against the Shares. The appeal focused on whether the Shares were the property of Botas or whether, as alleged by Botas, they were "the property of the State [ie Turkey]" under s13(2)(b) SIA, and hence immune from enforcement.

Ownership of assets, not purpose of use, is key question

Botas' first line of argument was that the "property of the State" should be interpreted by reference to whether the property was intended for commercial purpose as stated in s13(4) SIA (which operates as an exception to s13(2)(b)) (the **Commercial Exception**). The Privy Council disagreed. Whether assets are, in fact, the "property of the State" is a pre-condition to any consideration of whether the purpose of that property is commercial or sovereign. Otherwise, there would be no distinction between property owned by the State and that owned by SOEs in order to enable them to carry out their business. As the Shares are owned by Botas, and not Turkey, the Commercial Exception could not be applied.

"Property of a State" requires a proprietary or legal interest, not simply control or possession over the property

Botas' second line of argument was that "property" should be broadly interpreted to include, not only those assets in which the Turkish State enjoys a proprietary or legal interest, but also those over which it exercises significant control in terms of their use and disposition. Again, the Privy Council disagreed. For enforcement purposes, the nature of ownership of the "property of the State" means only a proprietary or legal interest; mere possession or control over the property will not be sufficient. There must be a realisable value in the property against which execution can be carried out.

In this case, the Shares were held by and for Botas in Jersey, subject to Jersey law, and were capable of disposal. The fact that, under Turkish law, the Turkish State had "control" over the Shares, consisting of rights and obligations placed on Botas which affected Botas' dealings with them, was irrelevant. The question of what constitutes "property" is a question for the court of the jurisdiction where enforcement is sought since enforcement only relates to property recognised as such under domestic law.

COMMENT

Although the question as to who owns the assets (the State or the SOE) is likely to be a fact-specific one, commercial parties seeking to enforce awards or judgments can now be more certain that assets (and particularly shares) owned by SOEs are unlikely to benefit from immunity from execution. However, although the decision provides clarity on the ability to execute awards against SOE assets, it remains the case that it is always advisable for commercial parties contracting with SOEs to attempt to negotiate written consent to enforcement/execution (in addition to submission to jurisdiction language). In particular, the commercial party should seek the SOE's consent to the enforcement of any order or judgment rendered in connection with any dispute arising out of the underlying contract, and to any relief granted by the English courts (including injunctions, specific performance and attachment). This may avoid an enforcing party having to go through the procedural and evidential hoops of establishing that the property against which enforcement is sought is indeed SOE property, rather than State property.

Stephanie Hawes
Associate
Litigation – Arbitration – London

Contact
Tel +44 20 3088 4968
stephanie.hawes@allenovery.com

Ram Mashru
Trainee
Litigation

Contact
Tel +44 20 3088 7152
ram.mashru@allenovery.com

Litigation Review consolidated index 2018

No contractual duty to protect spread betters against themselves: *Aryeh Ehrentreu v IG Index Ltd* (Feb)

Non-assignment clauses: what they do (and don't) restrict: *First Abu Dhabi Bank PJSC (formerly National Bank of Abu Dhabi PJSC) v BP Oil International Ltd* (Feb)

Widely drafted exclusion clause upheld: *(1) Interactive e-Solutions JLT (2) Interactive e-Solutions DMCC v O3B Africa Ltd* (Feb)

Non-reliance/advisory clause protects bank in swap misselling claim: *Marz Ltd v Bank of Scotland PLC* (Feb)

Contractual interpretation and implied terms: related contracts and limitations on confidentiality: *Kason Kek-Gardner Ltd v Process Components Ltd* (Jan)

Making a clean break – are your termination clauses sufficiently slick? *Monde Petroleum v Westernzagros* (Jan)

Crime

Cybercrime – remedies against unknown hackers: *CMOC Sales & Marketing Ltd v Person Unknown & 30 ors* (Nov)

Bank ordered to disclose Suspicious Activity Reports to customer: *Lonsdale v National Westminster Bank* (Nov)

ENRC v SFO appeal: internal corporate investigation documents were protected by privilege: *SFO v ENRC* (Sept/Oct)

SFO can request overseas documents from non-UK companies: *The Queen on the application of KBR Inc v The Director of the Serious Fraud Office* (Sept/Oct)

Failure to prevent bribery: guilty verdict in first contested case: *R v Skansen Interiors Ltd* (Mar)

Data Protection

Employer vicariously liable for rogue employee's data breach: *WM Morrison Supermarkets PLC v Various Claimants* (Nov)

Morrisons found vicariously liable for rogue employee's misuse of personal data: *Various claimants v Wm Morrisons Supermarket PLC* (Jan)

Disclosure

E-discovery – how to use predictive coding: *Triumph Controls UK v Primus International Holdings* (Mar)

Employment

Categorising worker status: *Pimlico Plumbers Ltd & anr (Appellants) v Smith (Respondent)* (July)

Restrictive covenants, Brexit, and the war for talent – why protecting your confidential information has never been more important: *Dyson Technology Ltd v Pellerey* (Jan)

Equity

Secured creditor has no absolute duty to preserve or maintain security for benefit of surety: *General Mediterranean Holding SA.SPF (aka General Mediterranean Holding SA) v Qucomhaps Holdings Ltd, William James Harkin (& anr)* (Nov)

Evidence

The inviolability of diplomatic mission documents: *R (on the application of Bancoult No. 3) v Secretary of State for Foreign and Commonwealth Affairs* (Mar)

Insolvency

MF Global CVA derailed by court order: *Heis & ors v Financial Services Compensation Scheme Ltd & anr* (July)

Portuguese bank resolution measures over English law governed loan: *Guardians of New Zealand Superannuation Fund & ors (Appellants) v Novo Banco SA; Goldman Sachs International v Novo Banco SA* (July)

Privilege

In-house counsel emails not privileged: *Glaxo Wellcome UK Ltd (t/a Allen & Hanburys) & anor v Sandoz Ltd & ors* (Nov)

Financial Reporting Council granted access to privileged documents of auditor's client: *FRC v Sports Direct International Plc* (Sept/Oct)

Legal advice privilege did not protect facts about client's assets: *Anthony David Kerman v Tatiana Akhmedova* (Mar)

No litigation privilege for controller of litigation under conduct of claims clause: *(1) Minera Las Bambas SA (2) MMG Swiss Finance AG v (1) Glencore Queensland Ltd (2) Glencore South America Ltd (3) Glencore International AG* (Mar)

Litigation privilege: applying the law post-ENRC: *Bilta (UK) Ltd (in liquidation) & ors v Royal Bank of Scotland Plc & anr and Health and Safety Executive, R. (on the application of) v Jukes* (Feb)

Procedure

Who has access to court documents? – the rules on non-party access: *Cape Intermediate Holdings Ltd v Mr Graham Dring (for and on behalf of the Asbestos Victims Support Group* (Sept/Oct)

Public law

Decisions of a private body acting as "skilled person" cannot be judicially reviewed: *R (Holmcroft Properties Ltd) v KPMG LLP & ors* (Nov)

Sanctions

Mere risk of exposure to sanctions insufficient for underwriters to avoid liability: *Mamancochet Mining Ltd v Defendants Managing Agency Ltd* (Nov)

Service

English court grants the European union summary judgment against Syria: *(1) The European Union (represented by the European Investment Bank) and (2) the European Investment Bank v the Syrian Arab Republic* (July)

Process agents – meaning of an "irrevocable" appointment: *Cargill International Trading PTE Ltd v Uttam Galva Steels Ltd* (Jun)

A new option for serving on a state?: *Koza Ltd & anr v Akcil & ors* (Mar)

Sovereign immunity

Assets owned by a state-owned enterprise not immune from enforcement: *Botas Petroleum Pipeline Corporation v Tepe Insaat Sanayii AS* (Nov)

Tort

Swap close-out costs – causation but no assumption of responsibility by auditors: *Manchester Building Society v Grant Thornton UK LLP* (Jun)

No parent company duty of care for Niger Delta claims: *Okpabi & ors v Royal Dutch Shell Plc & anr* (Feb)

Key contacts

If you require advice on any of the matters raised in this document, please call any of our partners or your usual contact at Allen & Overy.

Allen & Overy LLP

One Bishops Square, London E1 6AD, United Kingdom

Tel +44 20 3088 0000

Fax +44 20 3088 0088

allenovery.com