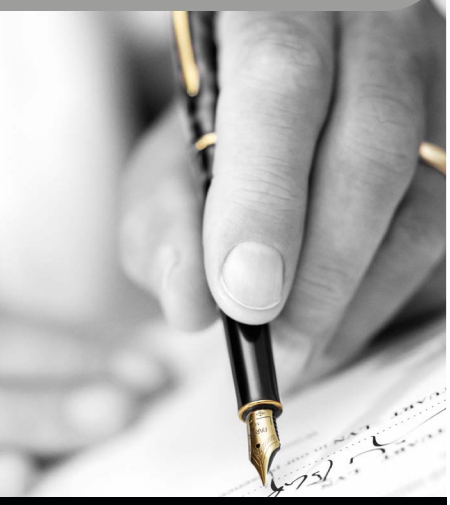
Corporate NEWSLETTER

Summer 2017

INSIDE THIS ISSUE:

EdwinCoe LLP

Charities & Philanthropy
Compliance & Regulatory Enforcement
Construction
Corporate & Commercial
Employment
Group Action Litigation
Immigration
Information Technology
Insurance Litigation
Intellectual Property
International
Litigation & Dispute Resolution
Private Client
Property
Property Litigation
Restructuring & Insolvency
Tax



Contents: Page

CORPORATE & COMMERCIAL LAW

The uncertainty of agreements to agree

Eoin Broderick, Associate

In a recent case between a shipping company and a shipbuilder, *Teekay Tankers Ltd v STX Offshore and Shipbuilding Co Ltd* [2017] EWHC 253 (Comm), an agreement granting the shipping company the option to purchase ships from the shipbuilder was ruled void for uncertainty by the High Court.

→

Editor's Note

Welcome to the Summer 2017 edition of our Corporate Newsletter which contains a variety of articles covering corporate & commercial, employment, property litigation, insurance litigation and intellectual property law.

I am delighted to announce that Edwin Coe received the *Rule of Law Award* at the Solicitors Journal Awards 2017 for our Brexit Article 50 challenge which was led by David Greene, our Senior Partner and Head of Litigation.

I can also confirm that in May 2018 we will be hosting the Annual General Meeting and client seminars for Ally Law, the global independent legal network that we are a member of. Further details will follow in our next edition.

If you have any legal issues or concerns that you would like to discuss, please do not hesitate to contact me.

Russel Shear
Head of Corporate & Commercial
t: +44 (0)20 7691 4082
e: russel.shear@edwincoe.com

Teekay Tankers (TT), the shipping company, claimed that STX, the shipbuilder, had renounced the option agreement (the "Agreement") and so, as they were entitled to under the Agreement, TT had terminated the Agreement and brought a claim for the loss of profits it would have earned if STX had complied with its obligations under it. STX's initial defence was that the Agreement was void for uncertainty as it was an agreement to agree.

There was no question that the parties intended to be legally bound by the Agreement but certain key terms had not been agreed. The Agreement provided that the delivery date of the ships was to be *"mutually agreed upon"* but that the shipbuilder would *"make best efforts"* to deliver the ships within a specified time period.

The Judge confirmed that the court will strive to find an implied term to save an agreement by lending it sufficient certainty. However, in accordance with *M&S v BNP Paribas* [2015] UKSC 72, the court will not imply a term where to do so would be inconsistent with express wording within the Agreement. TT asserted that it was an implied term of the Agreement that the date of delivery would either be such date as shall be offered by STX (having used its best efforts) or that it would be an objectively reasonable date (having regard to STX's obligation to use its best efforts), to be determined by the court if not agreed. The court disagreed with this suggestion and found that the suggested implied term that the delivery date would either be determined by STX, or would be identified by reference, to what is reasonable was inconsistent with the express clause requiring that the parties use their best efforts to agree a delivery date.

In reaching its judgement, the court confirmed the importance of the principles set out in *Mamidol-Jetoil Greek Petroleum Company SA v Okta Crude Oil Refinery AD* [2000] EWCA Civ 406 and *BJ Aviation Ltd v Pool Aviation Ltd* [2002] EWCA Civ 163 for analysing 'agreements to agree'. These principles, which should not be considered exhaustive, include:

- Each case must be decided on its own facts and the construction of the words used in that agreement.
- Where no contract exists, the use of the expression *"to be agreed"* in relation to an essential term is likely to prevent a contract from coming into existence on the grounds of uncertainty. Where a contract does exist, use of the expression *"to be agreed"* in relation to future executory obligations is not necessarily fatal to its continued existence.
- Where no contract exists, an absence of an agreement on essential terms of the Agreement may prevent any contract coming into existence on the grounds of uncertainty.
- Where there are commercial dealings between parties that are familiar with the trade in question and the parties have acted in the belief that there is a binding contract, the courts are willing to imply terms to enable the contract to be effective.
- Particularly in the case of contracts for future performance over a period, where the parties may leave matters to be adjusted in the working out of the contract, the court will assist parties to do so, so as to preserve rather than destroy bargains. This is particularly so, where one party already has the advantage of some performance which reflects the parties' agreement on a long-term relationship, or has had to make an investment premised on that agreement.
- For these purposes, an express stipulation for a reasonable or fair measure or price will be sufficient for the courts to act on. In the absence of express language, the courts are prepared to imply an obligation in terms of what is reasonable, as long as it is not inconsistent with express wording within the agreement.
- The presence of an arbitration clause may assist the court to hold a contract to be sufficiently certain.
- There is no obligation on the parties to negotiate in good faith about the matter which remains to be agreed between them.

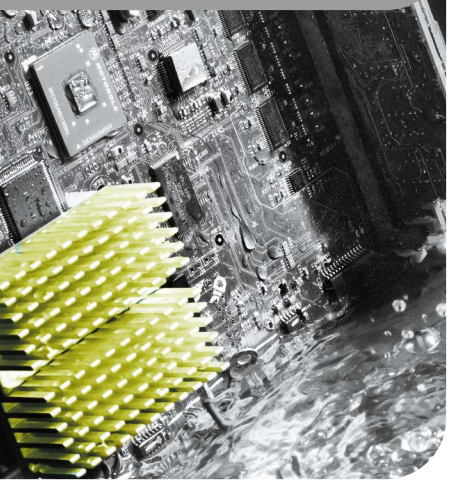
The key message from this case is that although it might be possible in some circumstances to imply terms to save an uncertain 'agreement to agree', it may not be enough to create a binding agreement where key terms remain to be agreed. It is safer to agree all terms of commercial contracts from the outset and avoid any risk that they may be found unenforceable.

"It is safer to agree all terms of commercial contracts from the outset and avoid any risk that they may be found unenforceable."

For further information with regard to this article, please contact:

Eoin Broderick
Associate
t: +44 (0)20 7691 4087
e: eoin.broderick@edwincoe.com

Or any member of the Edwin Coe Corporate & Commercial team



INSURANCE LITIGATION LAW

Cyber risk in the manufacturing industry

Nicola Maher, Partner

"Cyber-attacks or failures in the manufacturing IT system can lead to data manipulation that, if left undetected, may result in, for example, changes in product formulation or fundamental health and safety risks..."

As the cyber insurance market develops it is clear that the majority of cyber insurance is being purchased by those businesses at risk of data breaches, including retailers and financial services providers. However, data breaches, cyber-attacks and indeed IT system failures can affect any business in all industries and the manufacturing industry, which consists of companies in the automotive, aviation, construction, building materials, machinery and defence industries is far from immune.

Cyber-attacks and data breaches have been on the rise in the manufacturing industry in recent years. The fact that factories are increasingly computerised, automated and digitally integrated brings an increased vulnerability to cyber hacking, IT system failure and human error with resultant data breaches and the potential for physical damage, bodily injury and business interruption losses.

The current trend of automation and data exchange in manufacturing technologies is known as Industry 4.0. It includes cyber-physical systems, the internet of things and cloud computing. Industry 4.0 creates what is known as a smart factory in which cyber-physical systems monitor the physical processes of the factory and make decentralised decisions.

However, cyber-attacks or failures in the manufacturing IT system can lead to data manipulation that, if left undetected, may result in, for example, changes in product formulation or fundamental health and safety risks, in addition to intellectual property theft, loss of customer databases and deletion of critical data.

If, for example, a robot is hacked or suffers a technical fault a production line may be interrupted for hours or days at significant cost to the business. If an algorithm is wrong or IT systems fail global supply chains could be severely disrupted.

Industrial Control Systems (ICS) are prevalent in smart factories but are also found in the utilities sector, healthcare, transportation and even consumer appliances.

One particular incident was reported in 2014 when a German steel mill experienced a spear-phishing1 attack which enabled hackers to gain access to the corporate network and ultimately to the blast furnace control system disrupting it to such a degree that it could not be shut down resulting in extensive damage.

In 2015, security researchers managed to successfully breach Fiat Chrysler's in-car system, Uconnect, which allowed hackers to take control of a Jeep on the highway prompting the recall of 1.4 million vehicles in the United States. Remote hijack vulnerability can result in a hacker remotely operating the brakes or even shutting off the engine, the potential consequences of which are extreme.

→

For further information with regard to this article, please contact:

Nicola Maher
Partner
t: +44 (0)20 7691 4069
e: nicola.maher@edwincoe.com

Or any member of the Edwin Coe Insurance Litigation team

There are a number of examples of ICS attacks targeting electric, oil/gas and water utility systems, such as the Maroochy Shire incident in Australia in 2000 and the Ukrainian Power Grid cyber-attack in 2015. The Maroochy sewage system utilised a SCADA operating system which was hacked by a disgruntled former employee causing pumps to stop working, alarms to fail and about 200,000 gallons of sewage to flood vast areas destroying nature reserves and countless fish and wildlife.

In 2015, Ukraine hackers successfully compromised the information systems of three energy distribution companies temporarily disrupting electricity supply to the end consumers. This involved prior compromise of corporate networks using spear-phishing emails with malware and subsequent seizure of the SCADA control system allowing hackers to remotely switch substations off.

Clearly businesses in the manufacturing industry and those using industrial control systems need to take cyber-security seriously and part of the risk management process should be to consider cyber liability insurance cover. A growing reliance on cloud providers, greater sophistication of hackers globally and increasingly digitised systems means that all industries have an increased exposure to cyber incidents.

However, in the event of a cyber-attack that shuts down a factory, manufacturers may not be covered by existing property and liability policies which are not naturally designed to give true cyber cover and which also require physical damage before they pay out. Furthermore, traditional cyber insurance policies are often designed for data breaches but the fast-growing and serious threat to manufacturers is more likely to be an attack on the ICS or supply chain. The current policies may not be designed to cover those particular exposures which may involve property damage and bodily injury.

Coverage in the marketplace is currently very varied but cyber policies generally tend to include a mix of third party liability coverage for damages suffered by third parties due to loss of data and first-party coverage for response, remediation costs, fines and penalties.

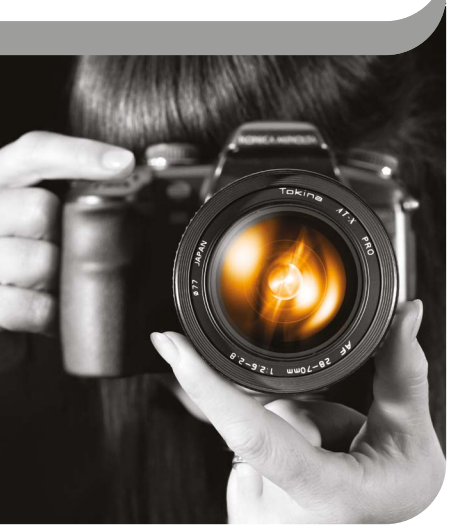
> "Clearly businesses in the manufacturing industry and those using industrial control systems need to take cyber-security seriously and part of the risk management process should be to consider cyber liability insurance cover."

I have set out below some key considerations for manufacturers to bear in mind when arranging adequate and appropriate insurance cover:

- **Determine the extent of cover required.** This will involve an assessment of potential financial and/or physical losses on a worst case/total loss basis and companies should assess their potential risks and exposures from cyber damage by carrying out a full cyber risk assessment. Critical business functions must be identified and a business continuity plan is essential.
- **Understand what is already covered within any existing policies, the extent of that cover and any exclusions that apply.** It is clear that the wording and exclusions of any existing general insurance policy should be carefully scrutinised to determine the level and extent of the protection it may offer in the event of a cyber loss. The interpretation of policy wording and exclusions both in general insurance and in stand-alone cyber policies may well become the subject of litigation in the event that insurance providers decline cover in the event of a loss. Until such time as insurers adopt standard form wording for cyber policies, policyholders are advised to consult with specialist insurance brokers and, where necessary, to seek legal advice in an effort to negotiate appropriate terms with insurers or to determine and understand the potential extent of cover in the event of a loss.
- **Ensure that any cyber insurance policy is drafted broadly** enough to capture both known and unknown future forms of cyber extortion or risk and is not limited only to named risks.
- **Particular attention should be paid to *"retention or waiting periods"*** which is the length of time for which the interruption must last in order to trigger business interruption cover. Many conventional insurance policies have waiting periods of 24 to 48 hours and typically cyber policies have waiting periods of around 6 to 12 hours. However, numerous businesses, including those in the manufacturing industry, may experience significant losses within minutes of a cyber loss occurring and it is important to consider with your broker whether the proposed waiting period is suitable for your business or whether a financial deductible is capable of agreement as an alternative.
- **Be aware of policy exclusions relating to IT systems.** For example, some cyber policies contain a *"failure to patch"* exclusion, which purports to exclude cover for losses attributable to a failure to install, or implement on a timely basis available software patches for known software vulnerabilities.

The cyber insurance market continues to evolve. Wordings have yet to be tested in court and it is clear that the scope of protection is also likely to change as insurers build up the available claims data. However, the potential for disputes is evident and businesses and their insurance brokers should be alive to the increasing need for cyber insurance cover.

Edwin Coe's specialist insurance lawyers act only for policyholders assisting and advising a wide range of corporate policyholders in relation to the adequacy and extent of existing cover. In addition to dealing with disputed insurance claims and coverage issues arising from denial of liability and policy avoidance insurers.



INTELLECTUAL PROPERTY LAW

Keep your PECR up! Emails about future marketing are marketing

Nick Phillips, Partner

"Flybe, may well be setting a trend that will continue as the General Data Protection Regulation (GDPR) comes into force and the ICO gets the power to fine a company €20 million or 4% of worldwide turnover (whichever is higher) for breaches of data protection legislation."

The Information Commissioner's Office (ICO) has served a timely reminder that when it comes to sending out electronic marketing (e.g. emails) it is important to consider whether the recipients of that marketing have previously notified you that they consent to receiving these communications from you. In this regard, emails which ask whether someone wants to receive marketing emails in the future, themselves count as marketing emails and should not be sent without the appropriate consent.

This is particularly important to bear in mind at a time when many organisations are looking to *"clean up"* their marketing lists in time for the General Data Protection Regulation (GDPR) to come into force in May 2018. As the ICO said, *"Businesses must understand they can't break one law to get ready for another"*.

ICO actions

In recent months, we have seen the ICO fine Flybe, Honda Europe, and Morrisons £70,000, £13,000, and £10,500 respectively for breaches of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

While these fines are rather modest given the size of the companies in question, and especially the egregious behaviour of Flybe, it may well be setting a trend that will continue as the General Data Protection Regulation (GDPR) comes into force and the ICO gets the power to fine a company €20 million or 4% of worldwide turnover (whichever is higher) for breaches of data protection legislation. The maximum fine at present is £500,000.

The acts which led to these ICO fines were in each case the contacting of large numbers of people from the companies' customer databases (sending 3.3 million, 300,000, and 130,000 emails respectively) asking the people to consent to future marketing. In Flybe's case, some of the people they sent the emails to had specifically opted out of marketing communications and in Morrisons' case, all of them had.

Honda's defence was that these emails were not themselves marketing, but were instead customer service emails to allow them to comply with the Data Protection Act 1998 (DPA), which requires that *"Personal data shall be accurate and, where necessary, kept up to date."* (DPA 1998, Schedule 1, Principle 4) and to ready themselves for the introduction of the GDPR. However, they could not produce evidence that their customers had given consent to this sort of communication, so the ICO found them to be breach of PECR.

For further information with regard to this article, please contact:

Nick Phillips
Partner
t: +44 (0)20 7691 4191
e: nick.phillips@edwincoe.com

Or any member of the Edwin Coe Intellectual Property team

PECR

PECR makes it much more difficult to send unsolicited electronic marketing and represents a considerably more prescriptive regime than that of the DPA. PECR does not, however, apply to non-electronic marketing (e.g. physical post) or marketing to legal persons (such as companies or LLPs). It also only applies to unsolicited communications, for example communications people have not asked to receive. In those circumstances you revert to the standards of the DPA and so, for example those engaging in non-electronic marketing are able to rely on the marketing being in their legitimate interests rather than just on the consent of the proposed recipients. This will remain the case after the introduction of the GDPR, but it will become more difficult to show that the necessary consent has been obtained, and therefore legitimate interest is likely to become all the more important.

Regulation 22(2) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 states the following:

Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender.

There is a very specific carve-out in Regulation 22(3):

A person may send or instigate the sending of electronic mail for the purposes of direct marketing where:

a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;

b) the direct marketing is in respect of that person's similar products and services only; and

c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication.

To comply with Regulation 22, the consent must be *"knowingly and freely given, clear and specific"*. It was the 'specificity' that tripped up Honda, as the ICO said that their customers had not given consent to the sort of marketing in question.

> "To comply with Regulation 22, the consent must be *"knowingly and freely given, clear and specific"*."

Practical considerations

- ***Where PECR applies***

  The easiest way to prove that you have received consent, as recommended by the ICO guidance on Direct Marketing [**https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf**] is to have the customer tick an opt-in box on your website. As the ICO says, there must be a:

  "Communication or positive action by which the individual clearly and knowingly indicates their agreement. This might involve click an icon, sending an email, subscribing to a service, or providing oral confirmation."

  As Flybe, Honda and Morrisons found to their cost, the ICO guidance goes on to say:

  "Note than organisations cannot email or text an individual to ask for consent to future marketing messages. That email or text is in itself sent for the purpose of direct marketing, and so is subject to the same rules as marking text and emails. And calls asking for consent are subject to the same rules as other marketing calls."

  In order to ensure that they do not fall into the same trap as Flybe, Honda and Morrisons organisations should keep a database of those individuals, sole-traders and partnerships whose data they hold and who have consented to receiving unsolicited direct marketing. Such databases need to record who has consented to what, how and when and should be maintained accurately and kept up to date bearing in mind that consent is unlikely to last forever. Unsolicited electronic marketing should then only be sent to those people who the organisation is confident and can prove have previously notified them that they consent to receiving these communications.

- ***Where PECR does not apply***

  For companies and LLPs who do not fall within PECR, it is also likely to be good practice to maintain a similar database recording what data has been collected, for what purposes and on what basis that processing can take place. Note that when the GDPR comes into force, the standard for consent will be higher (a freely given, specific, informed and unambiguous indication of his or her wishes is required and, for example, any kind of implicit or opt-out consent will for the most part not be sufficient). Therefore organisations will need to make sure that their databases only contain the information of people who have provided valid consent under the new regime, or satisfy themselves that they are covered by legitimate interest or some other ground which allows of processing. Given that the GDPR will be implemented in less than a year, this will be a mammoth undertaking for many organisations.

The team at Edwin Coe would be happy to advise on any concerns that you may have with regards to the data that you currently store or may store in the future.

EMPLOYMENT LAW

Indirect discrimination made simple?

Rachel Harrap, Partner

In the decision in the joined recent cases of *Essop and Naeem* [2017] UKSC 27, the Supreme Court undertook this daunting task: the simplification of indirect discrimination law.

Background

From what had become an area of law that was becoming increasingly tortuous and outcomes uncertain the decision in the above cases has produced a handful of principles which we believe purges the confusion and provides simplification of what had become complex and convoluted issues.

Direct discrimination – synopsis

Almost everyone has an intuitive understanding of direct discrimination. Direct discrimination is the less favourable treatment of an individual *"because of"* a protected characteristic, for example, sex, race or age. The characteristic must be the reason for the treatment. Put simply, whilst there are difficult cases, the core concept is easily understood. An employer has an express policy of refusing to employ women. In a case of that sort the discrimination is obvious. The employer treats women less favourably because of their sex.

There needs to be no context as the discriminatory impact of the criterion is apparent. The criterion is inherently discriminatory.

There is no defence where direct discrimination is established.

"There needs to be no context as the discriminatory impact of the criterion is apparent. The criterion is inherently discriminatory."

What makes indirect discrimination different?

Introducing and the *"context factor"*

To establish indirect discrimination there must be a practice, criterion or provision (PCP) that:

- puts one group at a disadvantage when compared to the others; and
- when applied, puts the individual at the same disadvantage as the group.

In essence, what can appear to be a neutral PCP when applied puts a group of persons sharing a protected characteristic at a disadvantage. Take by way of examples an employer that has as a PCP for employment a minimum height requirement. Unlike the policy in the direct discrimination example above, the PCP is not inherently discriminatory. It focuses on height, not sex. If men and women were on average the same height, this apparently neutral PCP would be neutral in its application. But men and women are not the same height on average. Women are, on average, shorter. Therefore the PCP will exclude more women than men. In order for the discriminatory impact of the PCP to be apparent, one needs context. In our example, the lower average height of women is what is identified in *Essop and Naeem* as a *"context factor"*. Indirect discrimination then occurs when the employer's PCP combines with one or more context factors to

→

produce a disparity of outcome between people with a particular protected characteristic and those who do not have it.

Context factors can come in many different forms. The height example is a genetic difference. A length of service PCP is well understood to discrimination against women. The relevant context factor is the social expectation that women will be the principal carers for children, which leads to a greater likelihood of career interruption.

These examples highlight two important things about context factors. First, they do not need to be in the *"control"* of the employer. It is not the employer's fault that women tend to be shorter, or that social expectation exists about childcare responsibilities. That is not to say that a context factor may not be within the employer's control. What is to be looked at is when the employer's PCP combines with a context factor, is the result an unequal playing field?

Where there is indirect discrimination there is the defence of justification if the employer can show that the application of the PCP is a proportionate means of achieving a legitimate aim. That is the employer must justify the use of the PCP.

It is important to understand that the context factor or factors is that they are always *"but for"* causes of the discriminatory impact. A height requirement would not be discriminatory if men and women were the same average height. A length of service PCP would not be discriminatory if men and women were equally likely to interrupt their careers to care for their children. Without the context factor, there is no discriminatory impact. The context factor is therefore always a cause. In the aforementioned cases, the Judge acknowledged this causal contribution by calling the context factor the *"reason for the disadvantage"*.

It is equally true, that the PCP is always a cause. Again, if there was no height requirement it does not matter if there is a difference in the average height of men and women. Similarly, if you avoid using a length of service PCP you avoid the discrimination that might otherwise occur.

Both the PCP and the context factor or factors are *"but for"* causes of the discriminatory impact. They both contribute to the uneven slope of the playing field.

Summary

The requirements required for indirect discrimination to arise:

- Is there a PCP?
- Is there a context factor?
- Do they combine to create a group disadvantage?
- Is the same context factor a cause of the individual disadvantage claimed?

If the answer to all four questions is yes, the employer should be made to justify the use of the PCP, even if there are other context factors in play otherwise indirect discrimination is made out.

If the Tribunal is satisfied that some other factor entirely explains the individual disadvantage, then the answer to the fourth question is no and a claim for indirect discrimination should fail.

"Both the PCP and the context factor or factors are "but for" causes of the discriminatory impact. They both contribute to the uneven slope of the playing field."

For further information with regard to this article, please contact:

Rachel Harrap
Partner
t: +44 (0)20 7691 4000
e: rachel.harrap@edwincoe.com

Or any member of the Edwin Coe **Employment team**

Latest News

Taylor's Modern Employment Practices – real change?

Employment Law

July saw the publication in the UK of Matthew Taylor's long awaited independent review into modern employment practices. The review sets seven principles for 'fair and decent work' and it is difficult to summarise in sound bites but the full list can be found on page 9 of the report, which is available to review here.

The one of particular interest is the 'renaming' of the current 'worker' status to 'dependent contractor' with the promise of clearer guidance on how to distinguish 'workers' from those who are genuinely self-employed.
To read the full article, please click here.

If you have any questions or comments about this topic please contact info@edwincoe.com.

PROPERTY LITIGATION LAW

Commercial rent deposits: what happens on insolvency of landlord or tenant?

Joanna Osborne, Head of Property Litigation

Landlords often require their tenants to provide a rent deposit as security for payment of the rent and performance of the tenant's covenants in the lease. The rent deposit deed will set out the circumstances in which the landlord can draw against this money and the conditions that must be satisfied for the deposit to be repaid to the tenant. Both landlords and tenants need to be aware of the implications of the other becoming insolvent in relation to the rent deposit funds.

"For protection from a situation where a tenant may become insolvent, the landlord should ensure that it has the benefit of a charge over the deposit money and is therefore a secure creditor."

Rent deposits as financial collateral arrangements

Up to 6 April 2013 rent deposit charges needed to be registered at Companies House within 21 days of creation in order to be valid. Since that date charges over rent deposits are no longer registerable security and cannot be registered at Companies House. Instead landlords and tenants need to pay attention to the charge structure itself to make clear that the deposit money should be safe from either the landlord's or the tenant's insolvency official.

Under the Financial Collateral Arrangements (No. 2) Regulations 2003, there are reduced formalities for the creation and registration of a rent deposit and improved enforcement rights. Since 6 April 2013, a rent deposit in a charging form will be construed as *"a Financial Collateral Arrangement"* if the rent deposit is entered into between two non-natural persons (not individuals).

The effect of the Financial Collateral Regulations 2003 on rent deposits since 6 April 2013 is as follows:

- There is now no need to register the deed at Companies House.
- Any moratorium on the administration or liquidation of the tenant will not apply and the landlord will be able to withdraw monies from the rent deposit without first seeking the agreement of the administrator, liquidator or the Court.
- As a liquidator has the right to disclaim a lease, if a rent deposit is included within the lease itself, this may automatically result in a disclaimer of the rent deposit. A liquidator will have no right to disclaim the rent deposit if this is in a separate deed.
- There will be no need for the landlord to get a Court Order to draw down the rent deposit.

Rent deposit structures

There are five main ways in which the rent deposit can be structured. Care needs to be taken in deciding which one depending on all the circumstances, including potential insolvency, the ease of operation, cost and tax considerations and the ability to transfer the rent deposit to successors in title. The five main ways of holding a rent deposit are as follows:

1. **The landlord holds the money, but it continues to belong to the tenant, who charges it in favour of the landlord.** This is the most common arrangement for holding a rent deposit.
2. **The tenant holds and owns the money, but charges it in favour of the landlord.**
3. **The landlord holds the money on trust for the tenant.**
4. **An independent third party, usually the landlord's solicitor or managing agent, holds the money as a stakeholder.**
5. **The money is paid to the landlord, belongs to the landlord and is either held as part of the landlord's general funds or in a separate account.**

Protection from landlord insolvency

Applying the different arrangements set out above for holding rent deposits:

1. Here the tenant should ensure that its name appears on the rent deposit account, in order to put the bank on notice that the funds do not belong to the landlord and to prevent a set off or combining of accounts. Also this will put the landlord's insolvency official on notice that some other party is interested in the money and there should be further investigation. As the owner of the deposit money, the tenant creates a fixed equitable charge in favour of the landlord as security for performance by the tenant of its obligations under the lease. The deposit money should be safe from the landlord's insolvency official, who would be bound to use it only in accordance of the terms of the rent deposit deed.
2. The deposit money belongs to and is retained by the tenant who deposits it in a separate bank account. The tenant creates a fixed equitable charge over the deposit money in favour of the landlord as security for performance by the tenant of its obligations under the lease. Keeping the deposit money in the tenant's own bank may help its relationship with its bank. The deposit money will be safe from the landlord's insolvency official. Interest on the account can be paid direct from the bank to the tenant.
3. As the deposit money is held by the landlord on express trust for the tenant, the landlord is the legal owner of the money, but is bound by the terms of the trust as to how it may use the money. The tenant retains the beneficial interest in the deposit money unless and until the landlord applies it in accordance with the term of the rent deposit deed. The deposit money will be safe from the landlord's insolvency official, because it does not become the landlord's own property as the landlord merely holds it as trustee. Care must be taken to ensure the landlord does not hold the deposit in one of its general accounts. As long as the money is held in a separate account, the landlord's bank will not be able to set off the funds in that account against any other debts or liabilities. The landlord is subject to fiduciary duties as a trustee and will be in breach of trust if it mixes the deposit money with its own monies.
4. The stakeholder, as an independent third party, acts as agent for both the landlord and tenant. This prevents the tenant's money from being mingled with the landlord's own funds and potentially lost to the tenant if the landlord becomes insolvent. Solicitors and managing agents are usually reluctant however to accept this type of continuing responsibility and may charge a fee for doing so.

International capabilities

An international member of

Ally Law

Ally Law's 2018 Annual General Meeting is now confirmed and will take place in London, UK on Wednesday 30 May 2018 to Saturday 2 June 2018. Further details will follow shortly.

Increasingly we find that clients' needs have an international dimension and we are able to offer access to Ally Law, of which we are a member. Ally Law is a group of independent law firms that provide comprehensive legal services worldwide.

We also have strong links in Russia, the Far East, the Middle East, and Sub-Saharan Africa, and regularly assist clients with global or pan-national businesses. We are able to provide legal services to an equal or higher standard than firms much larger than ourselves. This is demonstrated by the fact that we have won (and retained) tenders for the legal services of sizeable global companies in the face of competition from larger international firms.

If you have questions about how Edwin Coe and Ally Law can address your global business and legal needs, please contact Russel Shear, Head of Corporate & Commercial at Edwin Coe. Alternatively, please email team@ally-law.com.

5 This is an unattractive arrangement for a tenant, because the rent deposit is owned by the landlord with the monies being mingled with the landlord's own general funds. If the landlord becomes insolvent, the deposit money is indistinguishable from the landlord's other assets and can therefore be used by the insolvency official to meet claims from the landlord's general creditors. Also if the landlord owes money to the bank, that money can be set off in respect of the landlord's debts.

Rent deposits are therefore usually held in a charge rent deposit structure. A tenant will want to be named on the account so that the landlord's insolvency official will be on notice of the tenant's interest in the money.

Protection from tenant insolvency

If the tenant becomes insolvent it is important that the landlord can deduct unpaid rent and other overdue payments from the rent deposit with minimum delay and cost. In this situation the rent deposit is intended to provide protection for the landlord.

1. As the owner of the deposit money, the tenant creates a fixed equitable charge over it in favour of the landlord as security for performance by the tenant of its obligations under the lease, ensuring that if the tenant becomes insolvent the landlord is a secured creditor. Up until 6 April 2013, the rent deposit deed was unenforceable against a tenant's insolvency official if it was not registered at Companies House. Since that time, charges over rent deposit are no longer registerable security and cannot be registered at Companies House. If the tenant becomes insolvent, the landlord has the benefit of the charge and is a secured creditor, although if there is any money left over after the tenant's obligations have been satisfied through the rent deposit, then the balance of the deposit monies have to be returned to the tenant's insolvency official. Care must be taken on the transfer of the reversion to a new landlord when it may be necessary to take a new charge.
2. There is no need for any charge by the tenant in favour of the landlord and the landlord can make any necessary deductions from the deposit as trustee. This can save time and administrative trouble and cost in having to register the charge. The landlord has control over the account. There can be other reasons, for example tax considerations, for ensuring that it is made clear that beneficial ownership of the deposit money remains with the tenant. There is a possibility however that such a trust could be said to create an equitable charge, which would then require registration under Section 860 (7) (g) of the Companies Act 2006, or risk being void against the tenant's insolvency official. The landlord can be under implied fiduciary duties, including for example to earn a reasonable rate of interest on the deposit money and to account to the tenant for that interest.
3. As mentioned above this type of arrangement places a significant administrative burden on the solicitor or managing agent who are likely to want to charge a fee.
4. It can be advantageous for the landlord to hold the deposit monies in an account with its own general funds, particularly for an institutional landlord with many properties, as it lessens the burden of administering numerous separate rent deposit accounts.

For protection from a situation where a tenant may become insolvent, the landlord should ensure that it has the benefit of a charge over the deposit money and is therefore a secure creditor. Provided that the rent deposit is in the possession or control of the landlord, in the event that the tenant goes into administration or liquidation the landlord will be able to take money from the rent deposit in accordance with the terms of the rent deposit deed. The type of rent deposit arrangement used will therefore depend on the circumstances of each case.

Consider the terms carefully

Even if there is no immediate risk of insolvency, both landlords and tenants should consider the terms of a proposed rent deposit arrangement carefully, to ensure their position is protected.

"Even if there is no immediate risk of insolvency, both landlords and tenants should consider the terms of a proposed rent deposit arrangement carefully, to ensure their position is protected."

For further information with regard to this article, please contact:

Joanna Osborne
Head of Property Litigation
t: +44 (0)20 7691 4034
e: joanna.osborne@edwincoe.com

Or any member of the Edwin Coe Property Litigation team

We hope you find this newsletter useful and interesting, and we would welcome your comments. For further information and additional copies please contact the editor: Russel Shear on t: +44 (0)20 7691 4082 e: russel.shear@edwincoe.com

Edwin Coe LLP
2 Stone Buildings
Lincoln's Inn
London WC2A 3TH
t: +44 (0)20 7691 4000
e: info@edwincoe.com