WILLIAM FRY

LEGAL NEWS

Welcome

Welcome to the November issue of Legal News. For further information on any of the topics covered in this edition, please call or email any of the key contacts or your usual William Fry contact person.

Patricia Taylor

Partner

Court of Appeal Reverses Ruling that Directors Personally Liable for Debts Arising from Reckless Trading

The Court of Appeal has overturned a High Court ruling from 2015 that a former director of a car dealership was personally liable to a customer who paid the company for three vehicles in the weeks prior to the company's liquidation where the cars were ultimately not delivered to the customer due to the company's liquidation.

Background

The customer had agreed to purchase three vehicles from Appleyard Motors Limited (In Liquidation) ("Appleyard") and had transferred the full price of the vehicles to Appleyard's bank account. Appleyard sourced the vehicles through another car dealership, however, when Appleyard sought to transfer the funds to the other dealership its bank refused to facilitate the transfer. Consequently, the other car dealership refused to provide the vehicles to Appleyard and Appleyard was unable to deliver the vehicles to its customer. Appleyard sought to engage with its bank but having lost its support it ceased trading and went into liquidation shortly thereafter.

Appleyard had faced difficulties in the years leading up to its liquidation, including the withdrawal of a significant car stocking facility from a third party dealer. It was however established by the directors that they had obtained professional advice regarding the company's position, including the replacement of the stocking facility, and had secured a limited guaranteed stocking facility with the other dealership.

Following the commencement of the liquidation and the inability of the liquidator to return the funds to the customer, the customer brought an action to have the directors of Appleyard held personally liable for the company's debt. As previously reported here, the High Court found the directors guilty of reckless trading under Section 297(A) of the Companies Act 1963 and determined that they should be personally liable to the customer.

The appeal

One of the directors found to be personally liable appealed the decision to the Court of Appeal.

In overturning the High Court's decision, the Court of Appeal applied a modified form of the test under Section 297A to that applied by the High Court. The Court of Appeal held that having regard to the general knowledge, skill and experience that may reasonably be expected of a person in the position of the director, he ought to have known that his actions or those of

the company *would* cause loss to a creditor. It was not enough that, viewed objectively, the director ought to have known that his actions or those of the company *might* cause loss to a creditor.

The Court of Appeal held that the loss to the creditor must have been foreseeable to a high degree of certainty. Mr Justice Hogan, delivering the Court of Appeal's judgment, found that while it was clear that Appleyard's financial situation was perilous and it took an "*enhanced risk*" with the funds by accepting advance payment before the vehicles were delivered, the director had no reason to believe that the decision of the bank to cut off support to the company was imminent or even threatened. In such circumstances, the director could not have known that the receipt of the monies would cause loss to the customer and accordingly, it could not be held that the conduct of the director amounted to reckless trading for the purpose of ascribing personal liability under the Companies Act 1963.

Comment

The judgment appears to have vindicated the efforts of the directors to restructure the company in the period leading up to its liquidation. It is authority for the proposition that recklessness on the part of a director, for the purpose of holding that director personally liable for the debts of a company, will require knowledge that the actions of the director *would* in fact cause loss to creditors not that they *might* so do.

Contributed by Ruairi Rynn

Facebook not Obliged to Remove the Defamatory Posts of An Anonymous User

The High Court has ruled in *Muwema v Facebook Ireland* [*2016*] *IEHC 519* that the internet service provider was not obliged to remove the defamatory posts of an anonymous third party. The Court opted instead to exercise its discretion and made a Norwich Pharmacal order, forcing Facebook to reveal the identity of the user in question. Norwich Pharmacal orders are generally granted against a third party, forcing them to disclose information that assists the applicant in identifying and bringing legal proceedings against the individual who is believed to have wronged them.

Mr Muwema, a Ugandan lawyer (the "applicant"), initiated proceedings when a number of *"false scurrilous and defamatory*" comments were posted by a Facebook Ireland Limited ("Facebook") user operating under the pseudonym "TVO".

The case was brought in Ireland against Facebook as it is the contracting entity for users outside the US and Canada.

The applicant sought a number of interlocutory orders, namely:

1. An order prohibiting the publication or further publication of the posts
2. An order that Facebook or anyone on notice of the order cease and desist in further publishing the articles in question
3. An order directing Facebook to disclose the identity of TVO (a Norwich Pharmacal Order)

The reliefs sought at (1) above were refused by Justice Binchy who emphasised that the making of such an order would *"serve no useful purpose"* given that the information was now well within the public domain.

Justice Binchy also found that the prohibitory order sought at (2) above could only be available when the defendant had no defence which is reasonably likely to succeed and, in this instance, the defendant may well have been successful in availing of the "*innocent publication*" defence.

The applicant was successful, however, in obtaining a Norwich Pharmacal order compelling Facebook to disclose the identity of "TVO", the activist responsible for the defamatory publications.

The order, which is one of only a handful made in this jurisdiction, will now enable the applicant to pursue an action in defamation in Uganda against the user in question.

Contributed by David Cullen

Social Media Policy Put to the Test

The Employment Appeals Tribunal (EAT) recently found in favour of an employee who had been dismissed for breaching the company's social media policy due to the fact that the social media policy had not been properly implemented and not all employees were fully aware of it.

Background

This case involved an employee, who was employed by the employer as a driver until his dismissal on 13 February 2014 for gross misconduct.

The employee videoed one of the employer's trucks being incorrectly loaded and shared it on a chat forum specifically for car transportation drivers. The employer claimed that as this video would damage the company's reputation with clients, the action constituted gross misconduct. The employer also alleged that the employee had been reprimanded for a similar offence earlier in his career with the company and that he had broken the social media policy which was introduced as a result of that earlier offence. The employee argued that he had not received the social media policy due to a change in his address and that there was no reference to social media in the employee handbook.

Decision

The EAT awarded the employee €7,500. It determined that the impugned conduct was not in dispute and therefore the disciplinary procedures followed by the employer were correct but that because of the employee's good record and admission of responsibility his dismissal was disproportionate.

Comment

William Fry's Employment Snapshot 2016 – *Social Media in the Workplace*, highlights that as of May 2016, only 39% of employers in Ireland have a social media policy in place. This case reinforces the importance of social media polices and the need for a social media policy to be implemented carefully within companies. Companies should furthermore ensure that employees are made aware of the policy in their initial employment contract, that they are aware of their obligations under the policy and that they fully understand the policy.

Download your copy of the William Fry Employment Snapshot 2016 – Social Media in the Workplace

Follow us on Twitter @WFEmploymentlaw

Contributed by Catherine O'Flynn & Aedín Brennan

Practical Tips: Companies Registration Office Updates

Digital certificates for new companies

The Companies Registration Office (CRO) has started issuing digital Certificates of Incorporation for new companies as of 21 September 2016. These digital documents are replacing the paper Certificates of Incorporation which will be familiar to companies and their officers.

The digital Certificate of Incorporation will be emailed as a pdf document to the email address entered in the relevant section of the Form A1 following registration. The document will contain a coloured banner at the top to confirm that it has been digitally signed as certified by the CRO. The CRO has stated that this provides an assurance to the recipient that the document is authentic, has not been tampered with and has been independently verified as sourced in the CRO.

Companies can then provide these digital certificates directly to third parties (e.g. financial institutions) by email as required.

Mandatory e-filing for certain submissions

From 1 June 2017, mandatory electronic filing will apply to the following submissions to the CRO:

- Form B1: Annual Return (including financial statements and electronic payment)
- Form B2: Change of registered office
- Form B10: Change of director and/or secretary, or in their particulars
- Form B73: Nomination of a new annual return date

It is important that those responsible for making CRO filings on behalf of a company familiarise themselves with the new online process ahead of this deadline.

End of Companies Act 2014 transition period

Under the Companies Act 2014 (the "Act"), all existing private companies limited by shares must convert to one of the new company types (LTD or DAC) during the transition period which ends on 30 November 2016.

Companies that have not done so will be automatically converted to a LTD by the CRO on 1 December 2016. The estimated waiting period for the CRO to process a conversion to a DAC is 1 week at present. The waiting period to process a conversion to a LTD is significantly longer at 8 weeks, although this can vary depending on the application.

We recommend that a company be proactive as regards their conversion, rather than relying on the default conversion provisions in the Act. If a company automatically converts to a LTD, the memorandum and articles of association on the public record will be deemed to exclude the objects clause and any other provisions inconsistent with mandatory provisions of the Act. However, those provisions will not be physically redacted from the constitution as available on the CRO register, which may cause confusion.

In addition, if the company automatically converts to a LTD at the end of the transition period the directors will be in breach of their obligations under the Act, although this breach does not carry any specific sanction.

Companies should bear in mind that the effective date of conversion to a LTD or a DAC is the date the new Certificate of Incorporation is issued by the CRO and not the date on which the resolution sanctioning the conversion is passed.

For further information on the conversion process, please see our publication *The Companies Act - The New Forms of Limited Company and How to Convert* here.

Contributed by Aoife Kavanagh

First Money Laundering and Terrorist Financing National Risk Assessment for Ireland Published

On 7 October 2016, the Department of Finance and the Department of Justice and Equality published the first National Risk Assessment for Ireland (NRA) on money-laundering and terrorist financing (AML/CTF). The NRA is a detailed document and reflects a key objective of the inter-governmental Financial Action Task Force (FATF) to promote effective implementation of legal, regulatory and operational AML/CTF measures. The NRA also anticipates the Fourth Anti-money Laundering Directive (EU 2015/849) (AMLD4) which is required to become law in EU member states in June 2017. AMLD4 introduces a requirement for member states to identify, assess, understand and mitigate AML/CTF risks, related data protection concerns and to keep their assessments up to date. It is envisaged that the NRA will be kept updated.

The NRA includes a review of the risks present in sub-sectors within the Irish financial services industry including investment funds. The various sub-sectors were given risk ratings based on "residual risk" i.e. *"the residual risk after taking mitigants and other relevant factors into account"*. The report acknowledges that a higher risk rating does not necessarily indicate that there is low compliance within the particular sector, noting that: *"Some sectors will by their very nature or scale remain higher risk even with robust AML/CTF compliance, whilst others may remain unproblematic, despite potential vulnerabilities".*

Risk ratings were ascribed to 21 sub-sectors within the financial services industry including the following:

- **Retail banking – high risk rating** due to the nature, scale and complexity of the sector and its central role in Irish financial services, offering core banking services to a broad population and acting as a gate-way to the wider financial sector.
- **Non-retail banks – medium-high risk rating**. Non-retail banks have a global presence and the majority of business conducted by them is non face-to-face with the use of electronic commerce to complete transactions. The use of complex products may make it difficult to identify the ultimate beneficial owner and the source of funds. Notwithstanding this, certain non-retail banks provide lower risk services to lower risk customers, which brought the overall risk rating to medium high.
- **Life assurance – medium-low risk rating** because many of the products offered by the sector do not provide sufficient flexibility to be attractive to money launderers or terrorist financers, for example protection-only or pension products. The potential risks presented by higher risk products such as single premium products can be mitigated both by due diligence conducted at the outset of and during the business relationship.
- **Funds/fund administrators – medium-high risk rating**. Although the fund industry is not cash based it has a high geographical reach in terms of the jurisdictions into which funds are marketed and also in terms of non-Irish funds to which fund administrators may provide services. There are high volumes of subscriptions and redemptions associated with certain types of funds and as funds are usually marketed through distributors there is no direct business relationship with the underlying investor. There is also a high level of outsourcing and significant reliance on third parties to conduct customer due diligence.

The NRA is a very useful document and provides significant detail not just on Ireland's legislative, supervisory and enforcement architecture and environment in the area of AML/CTF, but also information, statistics and risk assessments of financial and non-financial businesses and professions in Ireland which are subject to AML/CTF obligations and which are at risk of AML/CTF vulnerabilities.

Contributed by Patricia Taylor

WADA Hacks Highlight Importance of Effective Cyber-Security and Data Protection Procedures

The publication by ‘Fancy Bears’ (a group of international hackers) of the World-Anti Doping Agency's (WADA) database serves as a reminder to large organisations to be vigilant of the importance of effective cyber security to ensure compliance with Data Protection laws.

This hack has seen private medical records of Olympic athletes, including the cyclist Bradley Wiggins and tennis star Serena Williams, brought into the public eye. Serious questions have consequently been raised about WADA's data protection policies, their processing and storage of personal information and their procedures surrounding data protection generally.

The hack revealed information relating to Therapeutic Use Exemption Approvals (TUEs), which allow athletes to take drugs for specific medical circumstances that would otherwise be prohibited uses. WADA's guidelines state that TUEs will only be retained for 8 years. The oldest of Bradley Wiggins' TUEs that was leaked is from June 2008. While it is not known when the hack took place, it was possibly outside of this 8 year retention period and accordingly concerns have been raised about WADA's adherence to their own guidelines.

In addition, the athletes themselves will obviously be concerned about the leak, many of whom have had their sensitive personal information published in contravention of their fundamental right to privacy. The right to privacy is protected by both the Irish Constitution and the European Convention for Human Rights.

The hacks have impacted on the reputation of many athletes and could potentially reduce their brand value. Taking these concerns together it could give rise to future litigation as athletes seek monetary compensation for the damage to their reputation.

It has been reported that the hacks occurred as a result of phishing emails into user accounts of the Anti-Doping Administration and Management System. This highlights the necessary attention that must be paid to effective cyber security procedures, training and risk management within organisations.

As WADA and other large sporting organisations are now required to retain substantial amounts of personal data about athletes it is of critical importance that internal procedures are reviewed on an ongoing basis in this increasingly regulated area of law.

Follow us on Twitter @WFIDEA

Contributed by Leo Moore

How Safe Are Your Secrets? Directive (EU) 2016/943 "EU Trade Secrets Directive"

With one in four European companies falling victim to at least one case of information theft in 2013, compared to 18% in 2012, Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (the "Directive") is a welcome step towards harmonised EU protection for sensitive business information. Prior to the enactment of the Directive, the lack of European guidance led to a fragmented and uncertain regulatory framework in Europe where trade secrets, unlike in the US, were not treated as intellectual property rights (IPR) in themselves.

Protection of "trade secrets"

The Directive prohibits the unlawful acquisition, use and disclosure of trade secrets.

The acquisition, use or disclosure of a trade secret will also be considered unlawful where the person knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who unlawfully used or disclosed the trade secret.

What type of information constitutes a 'trade secret'?

Article 2(1) defines a ‘trade secret’ as information which meets the following criteria:

1. It is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question
2. It has commercial value because it is secret
3. It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret

The 'trade secret' definition is derived from the World Trade Organisation's Art.39 (2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Despite the seemingly all-encompassing definition, it remains unclear whether protection is extended to information such as client lists or pricing structures that are commercially valuable but freely available to large numbers of staff within an organisation.

Prior to the Directive, Ireland has followed the approach of UK Court of Appeal case in Faccenda Chicken Ltd v Fowler ("Faccenda Chicken") when adjudicating on cases concerning the level of protection for confidential business information. In Faccenda Chicken, sales information pertaining to suppliers, contractors, distributors and pricing structures were not deemed to be trade secrets. The Court found that such information was 'readily accessible' to large numbers of company staff including sales managers and administrative staff dealing with the financial accounts and as such the employer had not taken sufficient steps to guarantee the confidentiality of the information in question.

Court procedure

The Directive also includes provisions to preserve the confidentiality of trade secrets in the course of legal proceedings. For instance the court can restrict access of any trade secret document or access to the hearing to a limited number of persons. This will offer some comfort to companies who may have been deterred in the past from enforcing their legal rights in court in case this in turn led to the trade secrets being disclosed to more people.

Effect of the Directive

In Ireland, companies and individuals already have recourse to the court to protect their confidential information under the law of equity. Accordingly, it is unlikely that the Directive will have significant impact on the protection of trade secrets in Ireland. Nevertheless, the new Directive is to be welcomed for the following reasons:

- The current law on confidential information has no statutory footing
- There is little harmonisation with respect to the law of confidential information
- The Directive does for the first time offer a de minimis degree of protection for trade secrets across the entire EU

However, businesses wishing to avail of the protection of the Directive must bear in mind the requirements to be fulfilled before a document will be classified as a trade secret and are advised to consider their options with regard to taking 'reasonable steps' to ensure their secrets remain secret even within the four walls of the business.

Follow us on Twitter @WFIDEA

Contributed by Colette Brady

In Short: Irish Bribery Law – Change At Last?

In a signal of its intent to bring about long overdue reform of anti-bribery and corruption laws in Ireland, the Government's Autumn Legislative Programme lists the Criminal Justice (Corruption) Bill for priority publication.

The general scheme of the Criminal Justice (Corruption) Bill was first published by the last Government in 2012 but its progress through the Oireachtas stalled.

While the final form of this Bill has yet to be confirmed, on the basis of the general scheme, the legislation is likely to have significant and far reaching implications for both doing business in Ireland and Irish businesses doing business abroad. If enacted, Irish citizens doing business abroad will be liable for prosecution for acts carried out abroad that fall foul of the legislation.

The legislation is intended to bring Ireland into line with international best standards in the area of combating bribery and corruption (both domestically and internationally) and has been broadly welcomed by Transparency International and the OECD.

A more detailed update will follow on the publication of the Bill.

Contributed by Gerard James

In Short: Employment-related Budget 2017 Announcements

Budget 2017 saw the announcement of a reduction to the three lowest Universal Social Charge (USC) rates by 0.5% (i.e. 1% rate cut to 0.5%, 3% rate cut to 2.5% and 5.5% rate cut to 5%). Incomes of €13,000 or less will remain exempt from USC. The banding ceiling for the reduced 2.5% rate of USC will increase to €18,772.

The minimum wage will increase by 10 cent per hour to €9.25 from January 2017. This increase had already been recommended by the Low Pay Commission.

Of interest to employers and employees alike will be the increase to the State pension of €5.00 per week from March 2017 and a Single Affordable Childcare Scheme which will take effect from September 2017. In summary, this scheme will involve parental means-tested subsidies of up to €80.00 per month or €900.00 per year for children aged 6 months to 15 years.

The Minister also indicated that an announcement will be made in Budget 2018 in relation to employee incentive schemes for SMEs.

Follow us on Twitter @WFEmploymentLaw

Contributed by Catherine O'Flynn and Nuala Clayton

In Short: William Fry Launches 'PrivacySource' – A Dedicated GDPR Implementation Resource

The long-awaited EU General Data Protection Regulation (GDPR) entered into force on 24 May 2016 and, following a two year transition period, will apply from 25 May 2018. Described as the most ground-breaking piece of EU legislation in the digital era, the GDPR aims to make businesses more accountable for data privacy compliance and offers citizens extra rights and more control over their personal data. The new rules will have significant impacts for all organisations.

In preparation for the application of GDPR, William Fry has launched "PrivacySource"; a dedicated website where our Technology team will provide ongoing analysis and assistance on the implementation of the GDPR. To gain access to this exclusive resource, we invite you to register here.

Contributed by John Magee