TECHNOLOGY
MEDIA & TELECOMMUNICATIONS

IN THIS ISSUE

VALIDLY CANCELLING OR AMENDING AN AGREEMENT VIA EMAIL IN SPITE OF A NON-VARIATION CLAUSE

Standard non-variation clauses in agreements seek to ensure that any variation or consensual cancellation of the agreement is formally agreed to by the parties, usually by requiring that such variation or cancellation be reduced to writing and signed by the parties. In a world where inter-party communication occurs mainly via email, the question arises whether an exchange of emails between the parties to an agreement would meet the standard requirements imposed by non-variation clauses.

This question was the subject of an appeal before the Supreme Court of Appeal (SCA) in the matter of *Spring Forest Trading v Wilberry (725/13 [2014] ZASCA 178 21 November 2014)*.

In summary, the facts of the matter were as follows: The appellant, Spring Forest Trading 599 CC (Spring Forest) and the respondent, Wilberry (Pty) Ltd (Wilberry) had entered into several agreements in terms of which Spring Forest leased certain mobile dispensing units from Wilberry for use in its car wash business. The agreements contained non-variation clauses which stated that "no variation … or agreement to cancel shall be of any force and effect unless in writing and signed by both you and us." After it became apparent that Spring Forest was not able to meet its rental commitments, the parties discussed a number of remedial options. Spring Forest opted to cancel the agreement and "walk away." The terms of the cancellation were recorded in emails exchanged between the parties in which the names of the parties appeared at the foot of the respective emails.

Spring Forest, believing that the agreements with Wilberry had been cancelled, entered into an agreement with another company to conduct the same business that had previously been conducted by Wilberry, in response to which Wilberry successfully launched proceedings in the court *a quo* and Spring Forest was interdicted from continuing its business under the new agreement.

Spring Forest lodged an appeal to the SCA on the basis that the agreements with Wilberry had been validly cancelled. The SCA held that the exchange of emails between the parties clearly and unambiguously demonstrated an intention by the parties to cancel the agreements concluded between them irrespective of a non-variation clause providing for cancellation to be in writing and signed by the parties.

In reaching its decision, the SCA examined the provisions of the Electronic Communications and Transactions Act, No 25 of 2002 (ECTA) which was enacted to "enable and facilitate electronic communications and transactions in the public interest." The SCA found that the requirement that the cancellation of the agreement be 'in writing' was satisfied by the chain of emails exchanged between the parties. Section 12 of ECTA provides as follows:

A requirement in law that a document or information must be in writing is met if the document or information is (a) in the form of a data message; and (b) accessible in a manner usable for subsequent reference.

With regards to the 'signed' requirement, the SCA had to consider whether the names of the parties at the foot of their respective emails constituted a 'signature' as contemplated by ss13(1) and 13(3) of ECTA. In this regard, it is important to note that ECTA differentiates between two kinds of signatures, namely (i) an "electronic signature" being "data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature," and (ii) an "advanced electronic signature" being "an electronic signature which results from a process which has been accredited by the [Accreditation] Authority as provided for in s37," and is normally used where the signature of a person is required by law and such law does not specify the type of signature to be used. In analysing the provisions, the SCA pointed out that s13 makes a distinction between a situation (i) where a law/statute requires a signature and (ii) where the parties themselves agree on the added formality of a signature. In the first instance, s13(1) of ECTA requires an advanced electronic signature whereas in the latter instance only an electronic signature is required as

continued

DLA CLIFFE DEKKER HOFMEYR

contemplated by s13(3) of ECTA. Having regard to this analysis, the SCA:

- rejected Wilberry's contention that an advanced electronic signature was required as the requirement for signature was agreed between the parties as a mere formality and not required by law/statute; and
- found that names of the parties at the foot of the respective emails constituted electronic signatures as envisaged in s13(3) of the ECTA on the basis that the names of the parties were intended to identify the parties and constituted 'data' that was logically associated with the data in the body of the emails and therefore constituted an electronic signature.

Contracting parties need to be cognisant of this judgment and carefully consider their communications with each other, particularly when using electronic means, including not only by emails but also via instant messaging platforms such as Twitter, Facebook, Instagram, BBM and the like. It is advisable for the parties to include express provisions in the contract which clearly regulate how electronic communications will apply in order to avoid disputes and ambiguity.

Simone Gill and Mukelo Ngobese

EMPLOYEES NOT LEFT IN THE COLD IN THE TERMINATION OF OUTSOURCED ARRANGEMENTS

There is no question that outsourcing is an effective service model which allows for core business focus and often results in reduced costs and improved efficiencies. Despite these advantages, the risks and practicalities associated with these arrangements cannot be overlooked and these should be comprehensively addressed in the agreement governing the outsource relationship so as to ensure that the parties rights are protected and there is an understanding of the implications of the arrangement, not only during its subsistence but also on termination.

A prevalent issue is that of the potentially significant impact of s197 of the Labour Relations Act, No 66 of 1995 on outsource transactions, both at the commencement of the arrangement and on termination. This issue has been under the spotlight and a wealth of precedents exist. The recent matter of *TMS Group Industrial Services (Pty) Ltd T/A Vericon vs Unitrans Supply Chain Solutions (Pty) Ltd and Others (JA58/2014) [2014] ZALAC 39 (6 August 2014)* which came before the Labour Appeal Court highlights the importance of being aware of the implications of s197 and including detailed provisions in outsource agreements to account therefor.

In this matter, Nampak Glass (Pty) Ltd (Nampak) outsourced its warehousing and distribution services to Unitrans Supply Chain Solutions (Pty) Ltd (USCS). The employees performing the services were employed by Unitrans Household Goods Logistics (Pty) Ltd (UHGL), a wholly owned subsidiary of USCS. The services were governed by a warehouse management agreement concluded between the parties on 1 February 2011. On expiry of the agreement on 31 January 2014, Nampak entered into a new agreement with TMS Group Industrial Services (Pty) Ltd t/a Vericon (Vericon) for the provision of warehousing and distribution services.

A dispute arose as to whether the employees of UHGL who were providing the services to Nampak under the previous agreement with USCS had been transferred to Vericon in terms of s197 as a result of the conclusion of the new agreement between Vericon and Nampak.

In resolving the dispute, the Labour Court (being the court of first instance) determined that there were essentially two issues that needed to be resolved. Firstly, whether the fact that the employees were employed by a different entity (ie UHGL) to the entity that contracted with Nampak (ie USCS), had any bearing on the application of s197 and secondly, whether the appointment of Vericon as the new service provider constituted a transfer of business as a going concern.

In addressing the first issue, the Labour Court referred to prior judgments handed down by the Constitutional Court as well as foreign jurisprudence in reiterating that s197 would apply to any transaction in terms of which the whole or part of a business is transferred as a going concern, irrespective of (i) the manner in which the transfer is occasioned and (ii) the 'generation' of the transfer. It held further that the employees that should transfer are the employees working in the business that is being transferred. These employees should transfer irrespective of who, in formal terms, is their employer. In addressing the second issue, the Labour Court pointed out that Nampak had provided USCS with the facilities, infrastructure and equipment that were necessary to perform the services (ie a comprehensive right to use of the assets), which constituted an economic entity for the purpose of s197 which afforded USCS, *inter alia*, the contractual right and practical

continued

ability to perform the services. When this contractual right was transferred to Vericon, it constituted a transfer of an economic entity which placed an obligation on Vericon to take transfer of the employees performing the services as well.

Accordingly, the Labour Court found that the termination of the agreement between USCS and Nampak and the conclusion of a new agreement for the provision of similar services between Nampak and Vericon constituted a transfer of a business as a going concern as contemplated by s197 and further, the employees who were employed by UHGL, had transferred to Vericon by operation of the law.

On appeal to the Labour Appeal Court (LAC), Vericon averred, inter alia, that it was merely providing a service to Nampak and that there was no transfer of the business as a going concern. Vericon submitted further that it had engaged its own resources in performing the services and did not take over any of the employees previously providing the services to Nampak, nor did it take over any assets, goodwill or intellectual property.

The LAC supported the decision of the Labour Court and held that in deciding whether a business has been transferred as a going concern, regard must be had to the substance and not the form of the transaction. In reaching its decision, the LAC took into account various factors including the following:

- the warehousing operation services were a discrete business;
- Vericon had assumed the right to use the same Nampak assets, computer systems, infrastructure, forklifts and other assets to continue to provide the same services to Nampak as those services that were previously provided by USCS;
- the services could only have been provided at Nampak's production facility; and
- the affected employees only performed services for Nampak.

The appeal was accordingly dismissed with the effect that Vericon was held to be the employer of the transferred employees by operation of law.

Although parties cannot contract out of statutory obligations, they can contractually provide for the steps to be taken and arrangements which will apply in the event of a transfer of employees by operation of law under s197. These steps may include agreeing on who will be responsible for costs, the conduct of the parties in respect of affected employees prior to termination/expiration and entering into arrangements with affected employees in anticipation of a s197 transfer.

Simone Gill and Mukelo Ngobese

SOUTH AFRICA: A HAVEN FOR CYBERCRIME?

The Whitehouse announced in the course of January of this year that President Barack Obama and Prime Minster David Cameron have agreed to cyberwar games to assist the United States and the United Kingdom in finding constructive ways to combat cybercrime. This comes on the back of statistics in the past few years which reveal a spike in the number of cybercrime incidents recorded globally. The Norton Report presented by Symantec in 2013 puts into perspective the global prevalence of cybercrime, reporting on more than 500 million victims that have been affected by cybercrime in a year, at the cost of more than US$113 billion to the global economy.

South Africa is not immune to this scourge. To the contrary, the same report ranked South Africa as the third highest country, after China and Russia, out of the 24 countries surveyed. The report's finding that 73% of South Africans in 2013 were victims of cybercrime is astounding and definitely a cause for concern.

The ubiquitous spread of cybercrime in South Africa is further evidenced by a report late last year from the Gautrain Management Agency that their financial department has been hacked in an attempt to defraud the agency of R800 million. Unfortunately news of this nature does not bode well for South Africa when considering how well-equipped we are to address cybercrime.

Chapter 13 of the Electronic Communications and Transaction Act, No 25 of 2002 (Act) provides the original framework created by the Department of Communications in relation to cybercrime. Notably, s86 of the Act strictly prohibits unauthorised interception of data. This section further criminalises the willful use of a device or a program to override

continued

any security systems meant to protect data and any violation of these provisions may result in criminal prosecution.

South Africa also adopted the National Cyber Security Policy Framework in March 2012, which seeks to define measures that are designed to address cyber threats at national level. The framework seeks to strengthen " intelligence collection, investigations, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber warfare, cyber terrorism and other cyber ills." The framework also introduces new institutional mechanisms to address cybercrime such as response committees and a cybercrime security hub.

Since the adoption of the framework little has been done, with the appointment of a National Cyber Security Advisory Council only taking place in October last year, some 18 months later.

The Police Minister also announced in October last year that a draft cybercrime policy and strategy had been drawn up in order to forge a national policy and strategic approach to fighting cybercrime. Industry experts have continued to express concerns regarding the lack of implementation.

When considering that a significant part of the defence budget in many nations is now being re-directed to assist with cybercrime initiatives, South Africa will need to rethink its own approach to ensure that it starts to develop the necessary skill set and mechanisms to address cybercrime, and prevent the risk of being a target for cyber criminals.

Tayyibah Suliman and Mulalo Tshikovhele

CONTACT US

For more information about our Technology, Media and Telecommunications practice and services, please contact:

Preeta Bhagattjee
National Practice Head
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@dlacdh.com

Simone Gill
Director
T +27 (0)11 562 1249
E simone.gill@dlacdh.com

Mukelo Ngobese
Senior Associate
T +27 (0)11 562 1374
E mukelo.ngobese@dlacdh.com

Tayyibah Suliman
Senior Associate
T +27 (0)11 562 1248
E tayyibah.suliman@dlacdh.com

Mariska van Zweel
Senior Associate
T +27 (0)21 481 6345
E mariska.vanzweel@dlacdh.com

BBBEE STATUS: LEVEL THREE CONTRIBUTOR

JOHANNESBURG
1 Protea Place Sandton Johannesburg 2196, Private Bag X40 Benmore 2010 South Africa
Dx 154 Randburg and Dx 42 Johannesburg
T +27 (0)11 562 1000 **F** +27 (0)11 562 1111 **E** jhb@dlacdh.com

CAPE TOWN
11 Buitengracht Street Cape Town 8001, PO Box 695 Cape Town 8000 South Africa
Dx 5 Cape Town
T +27 (0)21 481 6300 **F** +27 (0)21 481 6388 **E** ctn@dlacdh.com

cliffedekkerhofmeyr.com

DLA CLIFFE DEKKER HOFMEYR