18 FEBRUARY 2020

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS ALERT

Cybercrime in South Africa – attorneys fall victim to cyber fraud

The prevalence of cybercrime in South Africa is on the rise – confirmed by Acting Judge Klein in the recent judgment of *Fourie v Van Der Spuy and De Jongh Inc.* 2019 JDR 1801 (GP), who remarked on this while pronouncing on a case in which a law firm fell victim to hackers at the expense of their client.

That's the way the (Belgian) cookie crumbles – Belgian Data Protection Authority imposes a fine for the unlawful use of website cookies

In December 2019, a Belgian legal information company received an early Christmas present from the Belgian Data Protection Authority, namely a €15,000 fine for an insufficient cookie policy and consent mechanism on the company's website.

CDH
CLIFFE DEKKER HOFMEYR

CLICK HERE
FOR MORE INSIGHT INTO OUR EXPERTISE AND SERVICES

Cybercrime in South Africa – attorneys fall victim to cyber fraud

The Attorney paid the funds as instructed, without verifying the new banking details with the Applicant.

The prevalence of cybercrime in South Africa is on the rise – confirmed by Acting Judge Klein in the recent judgment of *Fourie v Van Der Spuy and De Jongh Inc.* 2019 JDR 1801 (GP), who remarked on this while pronouncing on a case in which a law firm fell victim to hackers at the expense of their client.

In the *Fourie* case, the client of a law firm (the Applicant) applied to the High Court seeking an order for damages against two practicing attorneys and their law firm (the Respondents) after one of the attorneys (the Attorney) had erroneously transferred the Applicant's funds out of the law firm's trust account and into several bank accounts held by one or more unknown hackers.

The Attorney had previously acted for the Applicant and was holding the funds in the law firm's trust account for the benefit of the Applicant, who had instructed the Attorney to retain the funds on his behalf. The Attorney subsequently received a number of emails purportedly sent from the email address of the Applicant, informing her of the "Applicant's" new banking details and instructing payment of the funds into a number of bank accounts. The Attorney paid the funds as instructed, without verifying the new banking details with the Applicant. It was only after the Attorney had transferred the funds into the new bank accounts that it was discovered that one or more unknown hackers had hacked the Applicant's email and provided the details of their own bank accounts – wherein the funds had erroneously been deposited by the Attorney.

The High Court said that "*[t]he [Attorney] was negligent and failed to exercise the requisite skill, knowledge and diligence expected of an average practicing attorney and thus failed to discharge her fiduciary duty to the Applicant by transacting via e-mail whilst full-well knowing that fraud is prevalent in her profession and not employing any measures to ensure that neither she, nor the Applicant will fall victim to fraud.*" The court rejected the Attorney's defence that a fraud had been perpetrated which had released her from her duty to account to her client, and concluded that the Attorney was, in fact, liable for her negligence. The Respondents were held jointly and severally liable for the loss suffered by the Applicant, with the High Court ordering the Respondents to pay the loss suffered by the Applicant over to the Applicant with interest.

Cybercrime in South Africa – attorneys fall victim to cyber fraud

...continued

Given the inadequacy of the current regulatory regime applicable to cybercrimes in South Africa, the Cybercrimes Bill is a beacon of hope for victims of cybercrime.

While the *Fourie* case primarily dealt with the principles concerning the nature of trust accounts and an attorney's duty of care owed to his/her client, it highlights the potential damage that can be caused by cyber criminals. Given the nature of cybercrimes, it is unfortunate that the victims of these crimes are forced to litigate against each other while the actual cyber criminals get away with the money! These injustices will, however, be addressed with the South African National Assembly having passed the Cybercrimes Bill of 2018 (B 6B—2017) (the Cybercrimes Bill) in November 2018. The Cybercrimes Bill (although not yet enacted into law) aims to criminalise both hacking and cyber fraud – two separate offences which the hackers in the *Fourie* case would potentially have been charged with had they been identified and subjected to investigation by the South African Police Services (SAPS). The offence of hacking (referred to in the Cybercrimes Bill as "*unlawful access*") carries a penalty on conviction of a fine (unspecified) and/or imprisonment for a period not exceeding five years whilst a conviction on a charge of cyber fraud grants the court a discretion to impose a penalty that it deems appropriate under section 276 of the Criminal Procedure Act 51 of 1977.

Given the inadequacy of the current regulatory regime applicable to cybercrimes in South Africa, the Cybercrimes Bill is a beacon of hope for victims of cybercrime such as the Applicant and the Respondents in the *Fourie* case. The enforcement of such law by the SAPS and prosecuting authorities (once the Cybercrimes Bill is enacted) will, however, be pivotal in bringing cyber criminals to justice.

Preeta Bhagattjee, Aphindile Govuza and Liam Sebanz

CDH
CLIFFE DEKKER HOFMEYR

That's the way the (Belgian) cookie crumbles – Belgian Data Protection Authority imposes a fine for the unlawful use of website cookies

Although the website users were primarily Dutch and French-speaking persons, the information on the company's website pertaining to the company's cookies was only available in English.

In December 2019, a Belgian legal information company received an early Christmas present from the Belgian Data Protection Authority, namely a €15,000 fine for an insufficient cookie policy and consent mechanism on the company's website.

The decision comes after the Belgian Data Protection Authority (Belgian DPA), on its own initiative, commenced an investigation into the offending company's cookie policy and mechanisms on its legal information website. In summary, the Belgian DPA made the following findings:

- the offending company's website did not contain sufficient information pertaining to both the types of cookies and the number of cookies which it deployed on its website;
- although the website users were primarily Dutch and French-speaking persons, the information on the company's website pertaining to the company's cookies was only available in English;
- the company's website did not contain an appropriate consent mechanism in terms of which the requisite consents for certain types of cookies which were used on the website could be obtained; and
- the website did not contain a simple mechanism in terms of which the website users could withdraw their consent to the use of cookies.

In view of the fact that the above decision was handed down pursuant to European data protection laws, it becomes necessary, from a South African law perspective, to consider the extent to which a South African website owner could potentially be held liable by the South African Information Regulator for a failure to implement and maintain an appropriate cookie policy and consent mechanism on its website. In this regard, it is relevant to note that the South African Protection of Personal Information Act 4 of 2013 (POPIA) does not contain express provisions which specifically regulate the use of cookies by South African website owners.

Notwithstanding the above, and considering the principle-based nature of POPIA, the following sections of POPIA will have a bearing on the data protection liability of website owners in relation to website cookies:

- section 11 of POPIA lists consent as a lawful basis upon which personal information may be processed. From a consent perspective, therefore, website owners utilising cookies on their websites should note that the utilisation of cookies (which collect the personal information of website users) constitutes the 'processing of personal information' under POPIA. Accordingly, website owners will need to ensure that appropriate consent mechanisms, which correctly facilitate a website user's giving and withdrawal of consent to the relevant cookies, be built into their website(s); and

That's the way the (Belgian) cookie crumbles – Belgian Data Protection Authority imposes a fine for the unlawful use of website cookies

...continued

Although POPIA is not yet fully in force and will only commence on a date to be determined by the President by proclamation in the Government Gazette, website owners are reminded that the office of the Information Regulator has already been established by the coming into effect of sections 39–54 of POPIA.

- section 19 of POPIA requires responsible parties to take appropriate and reasonable technical and organisational measures in order to prevent the unlawful processing of personal information. From an organisational security perspective, website owners must ensure that their cookie policies and statements which appear on their websites are, *inter alia*: (i) drafted clearly and concisely; (ii) drafted in plain and understandable language; (iii) specifically tailored to the website owner's business and processing activities; and (iv) sufficiently detailed with regard to the cookies which are used on their websites.

Although POPIA is not yet fully in force and will only commence on a date to be determined by the President by proclamation in the Government Gazette, website owners are reminded that the office of the Information Regulator has already been established by the coming into effect of sections 39–54 of POPIA. In this regard, the Information Regulator has, on occasion, proactively engaged companies in order to assist them in bringing their processing activities in line with the provisions of POPIA. In view of this practice, and in view of the impending commencement of the operative provisions of POPIA, website owners are advised to take measures to bring their website cookie policies, statements and consent mechanisms in line with the provisions of POPIA sooner rather than later.

Preeta Bhagattjee, Aphindile Govuza and Liam Sebanz

OUR TEAM

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

Christoff Pienaar
National Practice Head
Director
T +27 (0)21 481 6350
E christoff.pienaar@cdhlegal.com

Fatima Ameer-Mia
Director
T +27 (0)11 562 1992
E fatima.ameermia@cdhlegal.com

Preeta Bhagattjee
Director
T +27 (0)11 562 1038
E preeta.bhagattjee@cdhlegal.com

Simone Dickson
Director
T +27 (0)11 562 1249
E simone.dickson@cdhlegal.com

Aphindile Govuza
Senior Associate
T +27 (0)11 562 1090
E aphindile.govuza@cdhlegal.com

Nikita Kekana
Associate
T +27 (0)21 481 6334
E nikita.kekana@cdhlegal.com

Liam Sebanz
Associate
T +27 (0)11 562 1625
E liam.sebanz@cdhlegal.com

BBBEE STATUS: LEVEL ONE CONTRIBUTOR

Cliffe Dekker Hofmeyr is very pleased to have achieved a Level 1 BBBEE verification under the new BBBEE Codes of Good Practice. Our BBBEE verification is one of several components of our transformation strategy and we continue to seek ways of improving it in a meaningful manner.

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@cdhlegal.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@cdhlegal.com

STELLENBOSCH
14 Louw Street, Stellenbosch Central, Stellenbosch, 7600.
T +27 (0)21 481 6400 E cdhstellenbosch@cdhlegal.com