

DISPUTE RESOLUTION ALERT

IN THIS ISSUE

CORPORATE INVESTIGATIONS: THE HALLMARKS OF AN EFFECTIVE RMCP: SECTION 42 OF FICA

The Financial Intelligence Centre Act, No 38 of 2001 (FICA) and the Prevention of Organised Crime Act, No 121 of 1998 (POCA) are South Africa's cardinal pieces of legislation aimed at achieving compliance with its international obligations to combat, amongst others, money laundering and terrorist financing as well as strengthening financial systems against the threat of economic crime.

INSURERS USE THE F WORD TO BEAT FRAUD

Facebook, according to Statista, had 2.32 billion monthly active users by the fourth quarter of 2018. Thanks to Facebook, you can post videos, brag about your children, announce your new job or even moan about your former boss to people all over the world, instantly. Many people even have public profiles – meaning that they do not change their security settings to limit who can see what they post on Facebook – but do they know who's watching?

FOR MORE INSIGHT INTO OUR
EXPERTISE AND SERVICES

CLICK HERE 

CORPORATE INVESTIGATIONS: THE HALLMARKS OF AN EFFECTIVE RMCP: SECTION 42 OF FICA

On 2 October 2017, various amendments to FICA were enacted to align South Africa's anti-money laundering and counter terrorist financing laws with international best practise.

The risk-based approach is recognised internationally as the preferred approach to customer due diligence in various sectors including real estate, gambling, insurance, securities and banking.

The Financial Intelligence Centre Act, No 38 of 2001 (FICA) and the Prevention of Organised Crime Act, No 121 of 1998 (POCA) are South Africa's cardinal pieces of legislation aimed at achieving compliance with its international obligations to combat, amongst others, money laundering and terrorist financing as well as strengthening financial systems against the threat of economic crime.

On 2 October 2017, various amendments to FICA were enacted to align South Africa's anti-money laundering (AML) and counter terrorist financing (CFT) laws with international best practise. The amendments included a migration from the rules-based approach to the risk-based approach (RBA) to customer due diligence (CDD).

The RBA requires institutions to apply varied levels of due diligence commensurate to the degree of AML risk identified. Although there is no *numerus clausus* of risk categories, commonly identified risk categories include geographic, customer and product/service risk. As a result, by applying the RBA, institutions can direct their resources in a manner that is proportionate to the identified risk thereby promoting an efficient use of resources with minimal burden on their customers. It is also designed to afford institutions greater flexibility to use a wider range of mechanisms to achieve their know-your-customer (KYC) requirements, simplify their CDD measures in instances where a lower risk has been identified and provide

institutions with a greater discretion to determine the appropriate steps to be taken to ensure compliance with their internal AML and CFT rules. As a result, the RBA is recognised internationally as the preferred approach to CDD in various sectors including real estate, gambling, insurance, securities and banking.

Section 42 of FICA requires accountable institutions (AIs) to adopt a Risk Management and Compliance Programme (RMCP). This was required to be done by 2 April 2019. Implementation of an RMCP by AIs is critical to ensuring compliance with the RBA. The RMCP should include, amongst others, an AI's RMCP policy document, procedures, systems and internal controls directed at risk assessment and these should be tailored to the AI's particular business as no two AIs are likely to be the same. In the premise, a large AI which offers a wide range of services to a diverse client base would develop a more comprehensive RMCP in comparison to a smaller AI which offers a limited range of products to a smaller client base.



CLICK HERE to find out more about our Corporate Investigations team.

CORPORATE INVESTIGATIONS: THE HALLMARKS OF AN EFFECTIVE RMCP: SECTION 42 OF FICA

CONTINUED

The RMCP incorporates various aspects relating to customer identification and verification, ongoing and enhanced due diligence measures and record keeping.

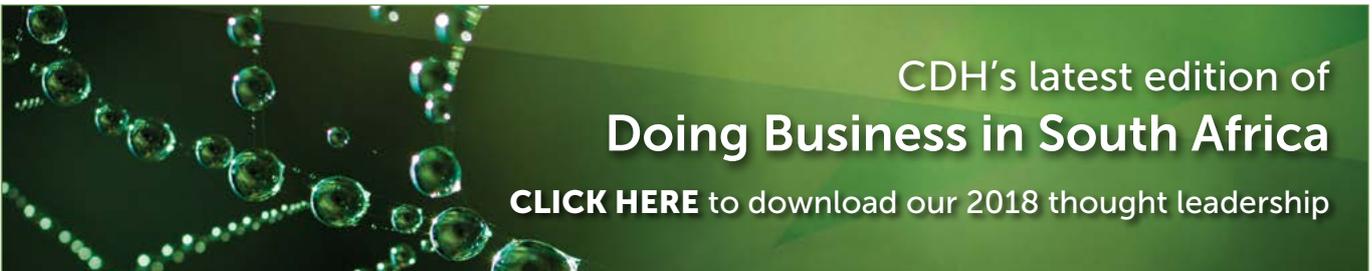


Section 42(2) of FICA requires the RMCP to enable AIs to, amongst others, identify and manage risk arising from the provision of its products or services. The RMCP incorporates various aspects relating to customer identification and verification, ongoing and enhanced due diligence measures and record keeping by specifying the way AIs must:

- determine if a person is a prospective client in the process of establishing a business relationship or entering into a single transaction or has already done so;
- comply with section 20A of FICA, which prohibits AIs from establishing a business relationship or concluding a single transaction with anonymous clients or a client with an apparent false name;
- establish and verify the identity of persons;
- determine whether future transactions are consistent with its knowledge of a prospective client;
- conduct additional due diligence measures in respect of legal persons, trusts and partnerships;

- conduct ongoing due diligence and account monitoring in respect of business relationships;
- examine complex or unusually large transactions and unusual patterns of transactions and keep written findings of the above;
- confirm information relating to a client when it has doubts about the veracity of information received;
- perform customer due diligence requirements when it suspects that a transaction or activity is suspicious;
- terminate existing business relationships;
- determine whether a prospective client is a foreign prominent public official or domestic prominent influential person;
- specify instances when simplified customer due diligence might be permitted; and
- maintains records as required by section 21 of FICA.

Section 42(2A) of FICA provides AIs with the discretion to indicate whether any of the above requirements do not apply to them. If this is the case, those AI's should provide reasons in their RMCP.



CDH's latest edition of
Doing Business in South Africa
CLICK HERE to download our 2018 thought leadership

CORPORATE INVESTIGATIONS: THE HALLMARKS OF AN EFFECTIVE RMCP: SECTION 42 OF FICA

CONTINUED

Section 42(2B) of FICA requires the board of directors, senior management or persons exercising the highest level of authority in an AI to approve the RMCP.



The RMCP must enable AIs to determine when a transaction or activity is reportable in terms of FICA as well as outline the processes for reporting such information. It must also provide for its implementation in the AI's branches, subsidiaries or foreign operations including the processes relating to implementation.

Section 42(2B) of FICA requires the board of directors, senior management or persons exercising the highest level of authority in an AI to approve the RMCP. Thereafter, AIs are, in terms of s42(2C), required to review their RMCP at regular intervals to ensure that it remains relevant to the AI's operations as well as compliance with FICA.

Although most AIs have existing mechanisms to assess risk in respect of potential and existing clients and transactions, those mechanisms may require further alignment to achieve compliance with the principles of the RBA. As a result, the successful adoption and implementation of an RMCP will require existing policies, procedures and internal controls to be streamlined into an RMCP that is tailored to the AI's operations and which approaches CDD measures in a manner that is proportionate to the identified category of risk.

Zaakir Mohamed and Krevania Pillay

CHAMBERS GLOBAL 2017 - 2019 ranked our Dispute Resolution practice in Band 1: Dispute Resolution.

CHAMBERS GLOBAL 2018 - 2019 named our Corporate Investigations sector as a Recognised Practitioner.

CHAMBERS GLOBAL 2018 - 2019 ranked our Dispute Resolution practice in Band 2: Insurance.

CHAMBERS GLOBAL 2018 - 2019 ranked our Dispute Resolution practice in Band 2: Media & Broadcasting.

CHAMBERS GLOBAL 2017 - 2019 ranked our Dispute Resolution practice in Band 2: Restructuring/Insolvency.

Julian Jones ranked by CHAMBERS GLOBAL 2017 - 2019 in Band 3: Restructuring/Insolvency.

Tim Fletcher ranked by CHAMBERS GLOBAL 2019 in Band 3: Dispute Resolution.

Pieter Conradie ranked by CHAMBERS GLOBAL 2019 as Senior Statespeople: Dispute Resolution.

Jonathan Witts-Hewinson ranked by CHAMBERS GLOBAL 2017 - 2019 in Band 2: Dispute Resolution.

Joe Whittle ranked by CHAMBERS GLOBAL 2016 - 2019 in Band 4: Construction.



INSURERS USE THE F WORD TO BEAT FRAUD

Insurance companies may use information found on a public Facebook profile.

Going back to insurance companies – are they allowed to use unlawfully obtained information?



Facebook, according to Statista, had 2.32 billion monthly active users by the fourth quarter of 2018. Thanks to Facebook, you can post videos, brag about your children, announce your new job or even moan about your former boss to people all over the world, instantly. Many people even have public profiles – meaning that they do not change their security settings to limit who can see what they post on Facebook – but do they know who's watching?

The Guardian newspaper recently reported that William Owen wasn't worried about who was looking at his profile. Mr Owen had come 7th out of 2,000 in a 10km race. Before that, he had signed up for a half marathon and posted a photograph of himself on top of Mount Snowdon. Who wouldn't plaster that all over Facebook? His insurer certainly "liked" his photos because the 29-year-old had, a few months earlier, claimed to have suffered neck and back pain caused by whiplash after a car reversed into his vehicle at a garage. His insurer understandably didn't think that they should have to pay his claim.

Insurance companies may use information found on a public Facebook profile. Yes, there is a right to privacy in s14 of the Constitution and it includes the right not to have your communication infringed but that right is not absolute. It is framed by subjective and objective expectations of privacy. When you click "I accept" on the standard terms and conditions on any social media platform you erode your own subjective expectation of privacy. Facebook, for example, expressly state in their Terms of Service that they "Provide a

personalised experience for you". How? By analysing "the connections you make, the choices and settings you select, and what you share and do on and off our Products". Your objective expectation of privacy requires the rest of society to recognise your expectation of privacy as being reasonable. So, if you are instagramming your dinners, tweeting your workout routine or vlogging about your online dating – society will assume that you aren't a very private person.

Facebook aside, to what other apps do you give personal information? Did you check their Terms of Service? The Wall Street Journal (WSJ) reported that several popular health apps share personal and health data with Facebook. Extreme Tech recounted a finding by WSJ that 11 of the 70 iOS apps it tested shared personal or health data with Facebook's servers via Facebook's Analytics. These included apps that record heart rate data or even when a user was having her period.

Going back to insurance companies – are they allowed to use unlawfully obtained information? For example, information obtained by hacking? Surprisingly, the position is not completely clear.

INSURERS USE THE F WORD TO BEAT FRAUD

CONTINUED

Should the rest of us have to pay higher premiums because Jane Soap faked a knee injury and then used her pay-out to go skiing? Surely not.



In *Harvey v Niland and Others*, Harvey relied on Niland's private Facebook posts to prove that Niland was secretly competing and violating his fiduciary duties to their joint business. Was the Facebook evidence admissible? Niland said it infringed his right to privacy and was obtained through the commission of an offence under s86(1) of the Electronic Communications and Transactions Act, No 25 of 2002 (Act). Judge Plasket held that the Act didn't prohibit evidence obtained in contravention of s86(1) but reasoned that the admission of the evidence would depend

- (i) on the nature and extent of the violation of Niland's right to privacy; and
- (ii) whether Harvey could have obtained the evidence in another, lawful way.

Judge Plasket found that hacking Niland's Facebook communications would have produced both information that was relevant to the issue before him and information that was irrelevant and entirely private. The relevant portion accessed established that Niland had been conducting himself in a duplicitous manner, contrary to the fiduciary duties he owed to the business – not to mention the fact that he had denied the allegations and undertaken not to do as he had done. Plasket said "his claim to privacy

rings rather hollow." Finally, the Judge found that the evidence was essential to Harvey's case and could not in practice have been procured in another, lawful way. "All he had was a suspicion but, without [the hacked posts], he had no evidence of Niland's wrongdoing." The application to strike out the hacked posts was dismissed with costs.

Arguably, an insurer can also rely on unlawfully obtained evidence to defeat a fraudulent claim. A fraudulent claimant is obviously acting dishonestly and what if that is the only way the insurer can prove it? Bhekisisa reports that fraud, waste and abuse is costing the private healthcare system more than R22 billion. In 2018, it was reported by IOL that by rooting out fraudulent claims, Discovery Health saved R568 million for its client schemes in 2017, up from R405 million in 2016. Should the rest of us have to pay higher premiums because Jane Soap faked a knee injury and then used her pay-out to go skiing? Surely not.

It is an intriguing debate, but in the meantime, you might want to re-evaluate your online and in app activity and decide what sort of privacy you expect to enjoy.

Tim Smit and Megan Badenhorst

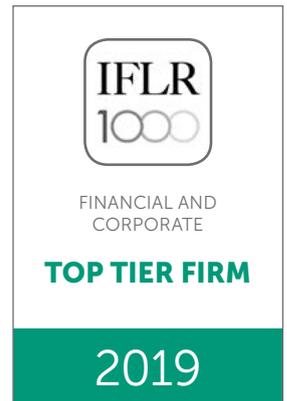


CLICK HERE to find out more about our Dispute Resolution practice.

CDH HAS BECOME THE EXCLUSIVE MEMBER FIRM IN AFRICA FOR THE:

Insuralex Global Insurance Lawyers Group
(the world's leading insurance and reinsurance law firm network).

[CLICK HERE TO READ MORE](#)



**Best Lawyers 2018 South Africa
NAMED CDH LITIGATION LAW FIRM OF THE YEAR**

Tim Fletcher was named the exclusive South African winner of the **ILO Client Choice Awards 2017 – 2018** in the litigation category.



OUR TEAM

For more information about our Dispute Resolution practice and services, please contact:



Tim Fletcher
National Practice Head
Director
T +27 (0)11 562 1061
E tim.fletcher@cdhlegal.com



Thabile Fuhrmann
Chairperson
Director
T +27 (0)11 562 1331
E thabile.fuhrmann@cdhlegal.com

Timothy Baker
Director
T +27 (0)21 481 6308
E timothy.baker@cdhlegal.com

Roy Barendse
Director
T +27 (0)21 405 6177
E roy.barendse@cdhlegal.com

Eugene Bester
Director
T +27 (0)11 562 1173
E eugene.bester@cdhlegal.com

Lionel Egypt
Director
T +27 (0)21 481 6400
E lionel.egypt@cdhlegal.com

Jackwell Feris
Director
T +27 (0)11 562 1825
E jackwell.feris@cdhlegal.com

Anja Hofmeyr
Director
T +27 (0)11 562 1129
E anja.hofmeyr@cdhlegal.com

Julian Jones
Director
T +27 (0)11 562 1189
E julian.jones@cdhlegal.com

Tobie Jordaan
Director
T +27 (0)11 562 1356
E tobie.jordaan@cdhlegal.com

Corné Lewis
Director
T +27 (0)11 562 1042
E corne.lewis@cdhlegal.com

Richard Marcus
Director
T +27 (0)21 481 6396
E richard.marcus@cdhlegal.com

Burton Meyer
Director
T +27 (0)11 562 1056
E burton.meyer@cdhlegal.com

Zaakir Mohamed
Director
T +27 (0)11 562 1094
E zaakir.mohamed@cdhlegal.com

Rishaban Moodley
Director
T +27 (0)11 562 1666
E rishaban.moodley@cdhlegal.com

Mongezi Mpahlwa
Director
T +27 (0)11 562 1476
E mongezi.mpahlwa@cdhlegal.com

Kgosi Nkaiseng
Director
T +27 (0)11 562 1864
E kgosi.nkaiseng@cdhlegal.com

Byron O'Connor
Director
T +27 (0)11 562 1140
E byron.oconnor@cdhlegal.com

Ashley Pillay
Director
T +27 (0)21 481 6348
E ashley.pillay@cdhlegal.com

Lucinde Rhoodie
Director
T +27 (0)21 405 6080
E lucinde.rhodie@cdhlegal.com

Belinda Scriba
Director
T +27 (0)21 405 6139
E belinda.scriba@cdhlegal.com

Tim Smit
Director
T +27 (0)11 562 1085
E tim.smit@cdhlegal.com

Willie van Wyk
Director
T +27 (0)11 562 1057
E willie.vanwyk@cdhlegal.com

Joe Whittle
Director
T +27 (0)11 562 1138
E joe.whittle@cdhlegal.com

Pieter Conradie
Executive Consultant
T +27 (0)11 562 1071
E pieter.conradie@cdhlegal.com

Willem Janse van Rensburg
Executive Consultant
T +27 (0)11 562 1110
E willem.jansevanrensburg@cdhlegal.com

Nick Muller
Executive Consultant
T +27 (0)21 481 6385
E nick.muller@cdhlegal.com

Jonathan Witts-Hewinson
Executive Consultant
T +27 (0)11 562 1146
E witts@cdhlegal.com

BBBEE STATUS: LEVEL TWO CONTRIBUTOR

Cliffe Dekker Hofmeyr is very pleased to have achieved a Level 2 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.

This information is published for general information purposes and is not intended to constitute legal advice. Specialist legal advice should always be sought in relation to any particular situation. Cliffe Dekker Hofmeyr will accept no responsibility for any actions taken or not taken on the basis of this publication.

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

©2019 7769/APR

