

# RISKALERT

MARCH 2023 NO 1/2022

## IN THIS EDITION

### RISK MANAGEMENT COLUMN

- Risk statistics paint a concerning picture

1

## RISK MANAGEMENT COLUMN

### Risk statistics paint a concerning picture

The Legal Practitioners Indemnity Insurance Fund NPC (LPIIF) had an outstanding reserve of R753, 343,300 as at 31 December 2022, a decrease of 2,2% from the corresponding figure as at the end of 2021. This figure represents the estimated value of outstanding claims notified to the company as at that date. As mentioned in previous publications, this is a significant number considering the nature and size of the LPIIF. Claims development patterns have remained stable over the last five years.

I will try to unpack some of the statistics in order to give an overview of the risks facing insured legal practitioners.

#### Claim trends

In the last five years, 59% of the claims paid by the LPIIF have arisen from prescription



Thomas Harban,  
Editor  
and General Manager  
LPIIF, Centurion  
Email: [thomas.harban@lpiif.co.za](mailto:thomas.harban@lpiif.co.za)  
Telephone: (012) 622 3928 or  
010 501 0723

related risks, with the prescription of Road Accident Fund (RAF) related claims making up 48% of the payments and general prescription (non-RAF) making up 11%. Other high-risk areas of practice are conveyancing (11%), under-settled RAF matters (10%), litigation (8%) and commercial matters (5%). The

**Legal Practitioners Indemnity Insurance Fund:** Thomas Harban, General Manager, 1256 Heuvel Avenue, Centurion 0127 • PO Box 12189, Die Hoewes 0163 • Docex 24, Centurion • Tel: 012 622 3900 Website: [www.lpiif.co.za](http://www.lpiif.co.za) • Twitter handle: @LPIIFZA

**Prescription Alert:** 2nd Floor, Waalburg Building, 28 Wale Street, Cape Town 8001 • PO Box 3062, Cape Town, 8000, South Africa, Docex 149 • Tel: (021) 422 2830 • Fax: (021) 422 2990 E-mail: [alert@aiif.co.za](mailto:alert@aiif.co.za) • Website: [www.lpiif.co.za](http://www.lpiif.co.za)

**Legal Practitioners' Fidelity Fund:** 5th Floor, Waalburg Building, 28 Wale Street, Cape Town 8001 • PO Box 3062, Cape Town, 8000, South Africa, Docex 154 • Tel: (021) 424 5351 • Fax: (021) 423 4819 E-mail: [attorneys@fidfund.co.za](mailto:attorneys@fidfund.co.za) • Website: [www.fidfund.co.za](http://www.fidfund.co.za)

**DISCLAIMER**  
Please note that the Risk Alert Bulletin is intended to provide general information to legal practitioners and its contents are not intended as legal advice.



**Legal Practitioners  
Indemnity Insurance  
Fund NPC**  
Est. 1993 by the Legal Practitioners Fidelity Fund



**LEGAL  
PRACTITIONERS'  
FIDELITY FUND**  
SOUTH AFRICA

## RISK MANAGEMENT COLUMN continued...

six main areas from which claims arise are consistent with previous years. Practitioners engaging in these high-risk areas of practice must put a significant amount of effort into their risk management measures.

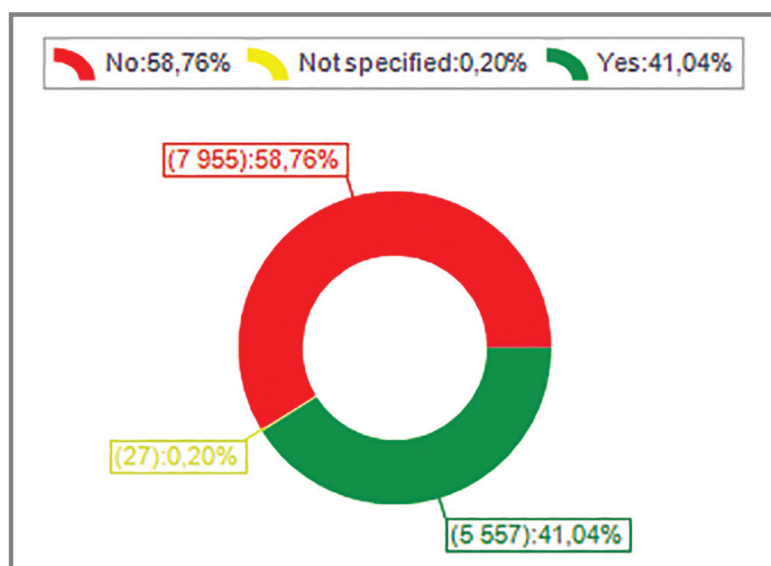
### Prescription

Prescription remains a major risk area despite the significant focus on this risk in our risk management education and publications. Unfortunately, some practitioners still do not recognise this as one of the main risks facing their practices.

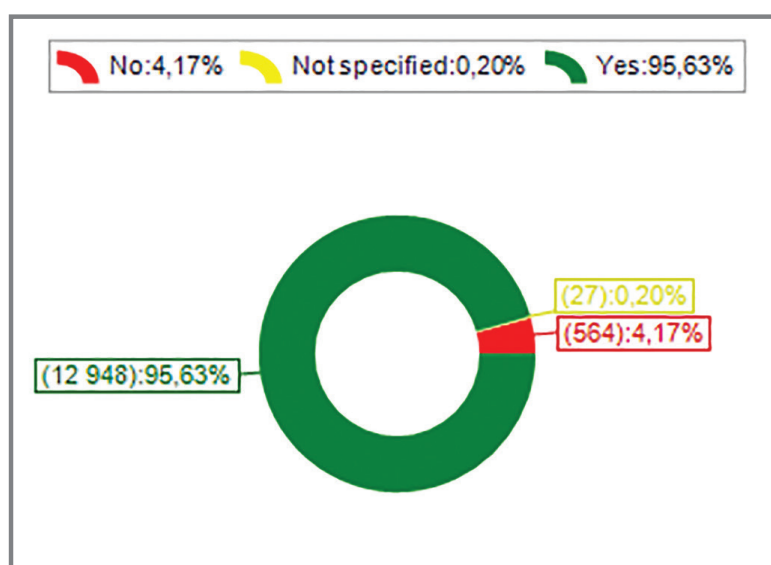
Some of the questions in the risk self-assessment questionnaire completed annually by practitioners are specifically focused on prescription. The graphs below give an overview of the responses provided in respect of each prescription related question.

One of the questions is: "Do you assess whether or not you have the appetite, resources and the expertise to carry out the mandate within the required time?" 98,53% of respondents replied in the affirmative to this question, with 1,26% replying in the negative and the remaining 0,21% not specifying whether or not they conduct the assessment.

### Has your firm registered all time-barred matters with the LPIIF's Prescription Alert unit?

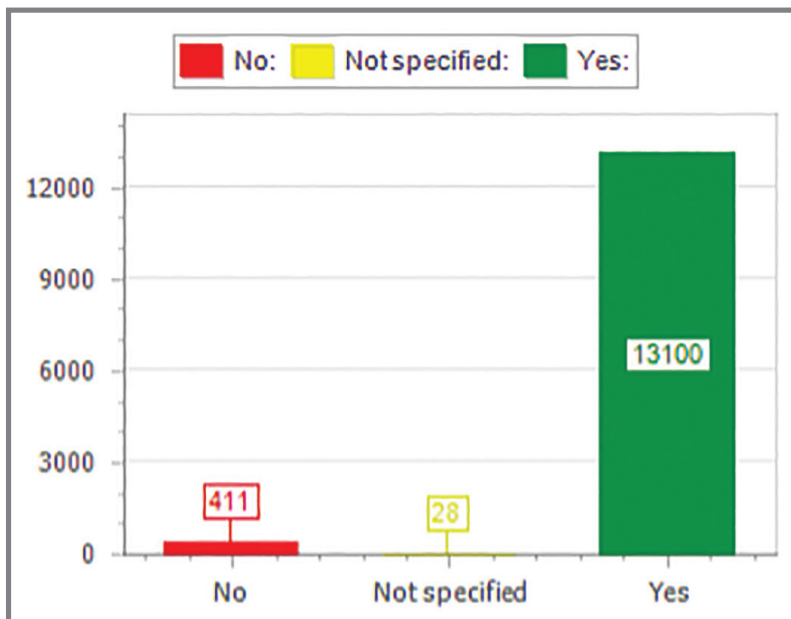


### Are regular file audits conducted?

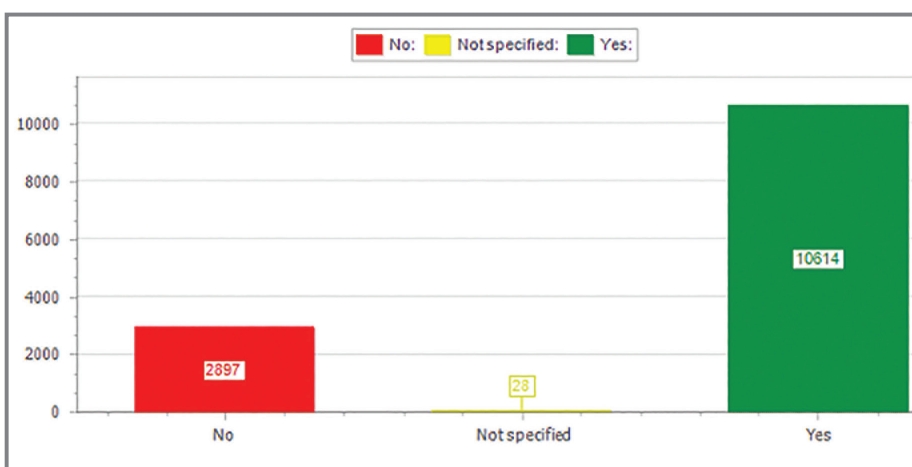


## RISK MANAGEMENT COLUMN continued...

**Is the proximity of the prescription date taken into account when accepting new instructions and explained to clients?**



**Do you have a formal handover process when a file is transferred from one person to another within the firm?**



The fact that less than 50% of practitioners have registered their time barred matters with the LPIIF's Prescription Alert unit is cause for concern. The Prescription Alert system is a back-up diary system made available by the LPIIF to insured legal practitioners at no cost. Our experience has shown that less than 10% of matters registered on the Prescription Alert system ultimately result in claims against the legal practitioners concerned. It is important that the correct information is uploaded onto the system when matters are registered so that the system can calculate the prescription date accurately. Reminders sent by the Prescription Alert unit of the looming prescription date must be adhered to.

Almost 97% of respondents completing the risk management self-assessment questionnaires indicate that the proximity of the prescription date is taken into account when accepting new instructions and is explained to clients, with almost 95% reporting that regular file audits are conducted in their practices. If this was indeed the case, the number and value of prescription related claims would have been much lower.

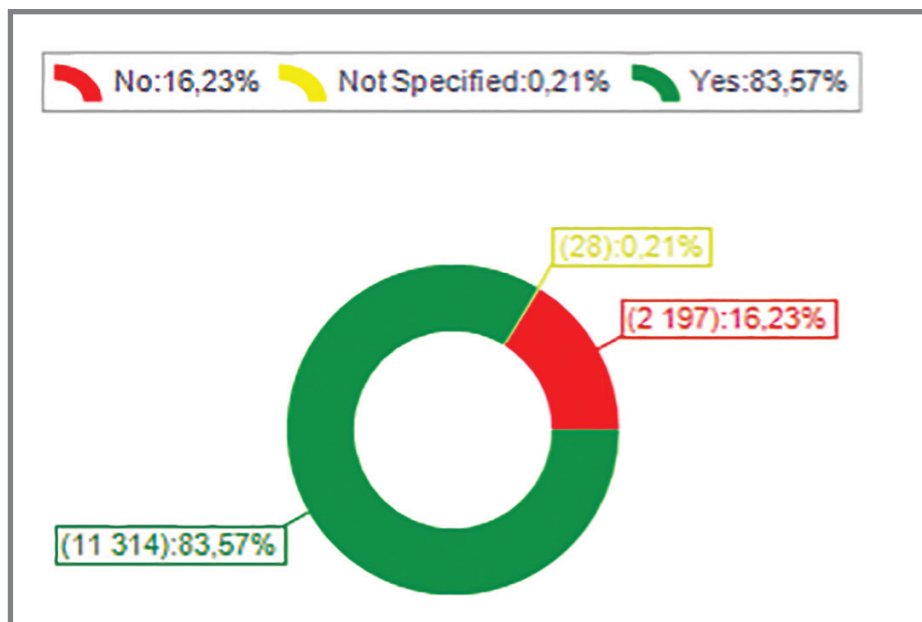
When faced with a special plea of prescription, do not concede if

## RISK MANAGEMENT COLUMN continued...

there are facts and legal grounds on which to replicate and challenge the prescription defence. It is thus important that you and your staff know the law regarding when the running of prescription commences, is suspended or interrupted. It is also concerning that more than 18 months after the judgement was handed down in the LPIIF's favour in *Legal Practitioners Indemnity Insurance Fund NPC v The Minister of Transport and The Road Accident Fund (GP)* (unreported case no 26286/2020, 21-6-2021) (Janse van Nieuwenhuizen J), some legal practitioners are still not challenging the RAF where the latter raises a special plea of prescription in respect of claims arising from accidents where the identity of the driver or the owner of the vehicle is not known (commonly referred to as 'hit and run' claims). The LPIIF successfully challenged the constitutionality of the RAF regulations setting the two-year prescription period for those claims. A copy of the judgment can be obtained from the LPIIF website or by sending your request to [risk.queries@lpiif.co.za](mailto:risk.queries@lpiif.co.za)

The recent Supreme Court of Appeal judgment in *Shoprite Checkers (Pty) Ltd v Mafate* (903/2021) [2023] ZASCA 14 (17 February 2023) gives some significant insight into the le-

### Does your practice have regular meetings of professional staff to discuss problem matters?



gal principles relating to prescription.

### Reasons for the questionnaire

One of the reasons for the introduction of the risk management self-assessment questionnaire was to focus the minds of legal practitioners on risk management and the internal controls that must be implemented in their practices. Providing inaccurate information when completing the questionnaire benefits neither the legal practitioners concerned nor the LPIIF. Legal practitioners should take time to go through the ques-

tionnaire and to provide considered and accurate answers. You will also get more value out of the exercise if you consider the aims with which it was introduced which are to:

- assist the LPIIF when setting and structuring excesses and amounts of cover for the profession as a whole, deciding on policy exclusions, conditions and possible premium setting;
- raise awareness regarding risk management and to get practitioners to think about risk management tools/procedures for their practices;

## RISK MANAGEMENT COLUMN continued...

- obtain relevant and usable general information and statistics about workloads, staff numbers, types of matters dealt with, stress levels, risk management/practice management and claims history;
- gain insight into which risk management/practice management procedures are in place/need to be put in place in practices;
- assist in the selection and formulation of the most effective risk management interventions; and
- assist in formulating a strategy to improve risk management/practice management at all levels.

Unfortunately, some practitioners only complete the questionnaires in order to comply with the LPIIF's Master Policy provisions and to meet the requirements of applying for a Fidelity Fund certificate. We are also aware that in some firms the completion of the questionnaire is delegated to administrative or support staff who may not have an appreciation of the importance of the risk management assessment. Those firms will not get the benefit of the risk management self-assessment process. Compare what information is provided in your risk assessment questionnaire to that provided by you in other areas, such as the proposal form that you

have completed when applying for or renewing your top-up insurance. Any incorrect information provided in respect of any question will not only be unethical but will also jeopardise your insurance cover. In the event that you are involved in litigation or some other dispute, it may be necessary to produce the documents. You should also compare your responses provided in the current year to those in prior years in order to assess how your risk management measures have progressed. If you handed each person in your firm a copy of the questionnaire to complete, how would the responses compare to that which you have submitted?

### The RAF

The implementation by the RAF of Board Notice 271 of 2022 on 4 July 2022 raised the bar significantly in respect of substantial compliance with the minimum requirements for the acceptance of claims. We have received numerous correspondence from members of the profession who are facing challenges with the RAF in this regard. The implementation of the Board Notice does not appear to be consistent across all RAF offices from what we can gather from the information received from the profession. We have also been made

aware of the fact that RAF offices are turning some claimants away at the door and not providing any written reasons for refusing to accept claims. These developments have a significant impact on the rights of RAF claimants and also increase the risk of prescription of RAF matters in the hands of attorneys.

The LPIIF has launched an application to review and set aside Board Notice 271 of 2022. At the time of writing, we are awaiting a complete record from the RAF. If you require a copy of the LPIIF's papers, please send a request to [risk.queries@lpiif.co.za](mailto:risk.queries@lpiif.co.za). Parties with an interest in the matter are urged to consider their positions and, if necessary, file applications to participate in review application. We anticipate that the review application will be heard in the latter part of 2023, at the earliest. In the interim, legal practitioners must do their best to comply with the Board Notice. The related matter (*Mautla and Others v RAF and Others*) will be argued on 9 May 2023. The review application in the *Mautla* matter concerns Board Notice 58 of 2021, the predecessor of Board Notice 271 of 2022.

### Cybercrime

The recent judgments in *Hawarden v Edward Nathan Sonnenbergs*



## RISK MANAGEMENT COLUMN continued...

Inc (13849/2020) [2023] ZAGPJHC 14 (16 January 2023) and *Hartog v Daly and Others* (A5012/2022) [2023] ZAGPJHC 40 (24 January 2023) have received a lot of media attention and generated much discussion regarding cybercrime. It is hoped that there will also be an increased awareness of cyber risks by law firms, their clients and other stakeholders in the wake of these judgments and the conversations that they have generated.

It will be remembered that cybercrime related claims are excluded from the LPIIF policy. Cybercrime is defined in the LPIIF policy as follows:

“IX **Cybercrime**: Any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the internet or any one or more of them. (The device may be the agent, the facilitator or the target of the crime or offence). Hacking of any of the electronic environments is not a necessity in order for the offence or loss to fall within this definition;”

The full wording of the exclusion clauses relevant to the cybercrime exclusion read as follows:

### “WHAT IS EXCLUDED FROM COVER?”

16. This policy does not cover any liability for compensation:

...

(c) which is insured or could more appropriately have been insured under any other valid and enforceable insurance policy available to the **Insured**, covering a loss arising out of the normal course and conduct of the business, or where the risk has been guaranteed by a person or entity, either in general or in respect of a particular transaction, to the extent to which it is covered by the guarantee. This includes but is not limited to Misappropriation of Trust Funds, Personal Injury, Commercial and **Cybercrime** insurance policies;

...

(o) arising out of **Cybercrime**. Losses arising out of **Cybercrime** include, payments made into an incorrect and/fraudulent bank account where either the Insured or the other party has been induced to make the payment into the incorrect bank account and has failed to verify the authenticity of such bank account;

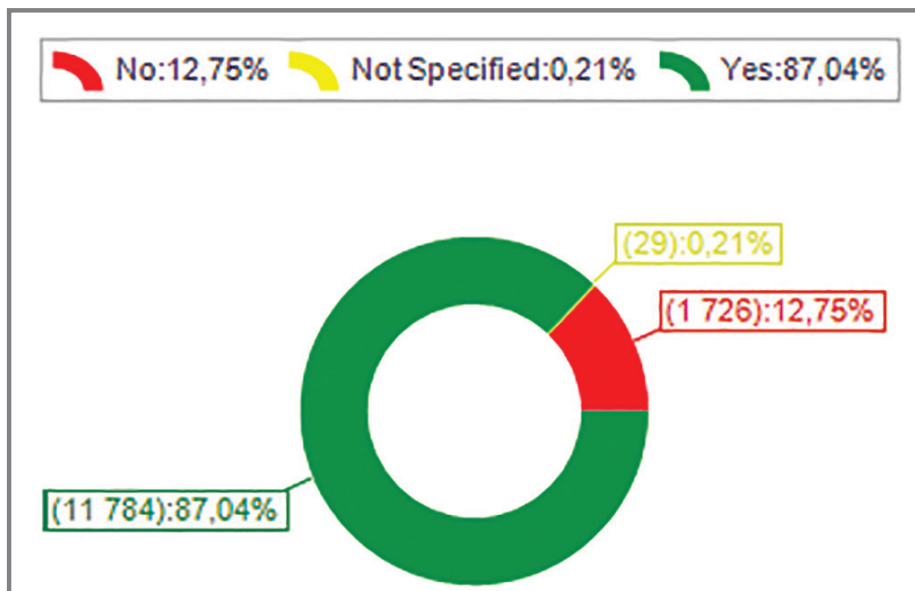
For purposes of this clause, “verify” means that the Insured must have a face-to-face meeting with the client and/or intended recipient of the funds. The client (or other intended recipient of the funds, as the case may be) must provide the **Insured** with an original signed and duly commissioned

affidavit confirming the instruction to change their banking details and attach an original stamped document from the bank confirming ownership of the account.”

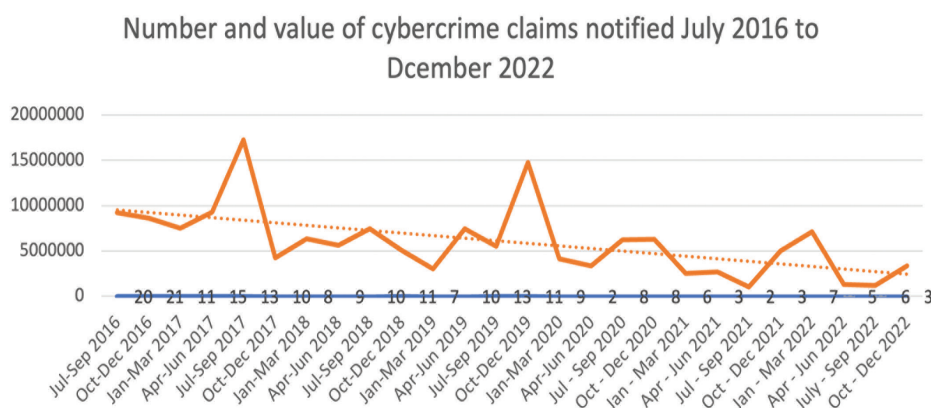
Between 1 July 2016 and 31 December 2022, the LPIIF was notified of 231 cybercrime related matters with a total value of R155,688,572.24. The average value of the cybercrime related claims is R5,988,022.01. All of these claims were not indemnified by the LPIIF as they fell within the exclusion clauses referred to above.

Cybercrime related claims are one of the most common type of claim notified to the LPIIF but excluded as they are not indemnified by the Master Policy. It is surprising that many practitioners still notify the LPIIF of cybercrime related matters when such claims have been excluded from the LPIIF policy since 1 July 2016 and there has been a lot of information directed to the profession regarding this exclusion. Moreover, almost 88% of practices have indicated that they have read the LPIIF Master policy and are aware of the exclusions. The question posed in the risk management self-assessment form asks: “Have you read the Master Policy and are you aware of the exclusions?” The statistics for the responses are as follows on page 7:

## RISK MANAGEMENT COLUMN continued...



**The pattern in respect of the cybercrime notifications will be gleaned from the graph below:**



The most common type of cybercrime notifications relate to firms that have fallen victim to what is now commonly referred to as business email compromise scams. This scam involves the receipt of an email from an imposter, purporting to be from the intended recipient of funds, fraudulently instructing a party to make payment into a bank account held by or controlled by the imposter. The verification of bank accounts and instructions to make payment into such bank accounts is one measure that can be implemented by parties to mitigate the risk of falling prey to business email compromise scams. Practitioners must also have regard to the steps suggested in the judgments handed down in *Hawarden v Edward Nathan Sonnenbergs Inc, Jurgens and Another v Volschenk* (4067/18) [2019] ZAECPEHC 41 (27 June 2019) and *Fourie v Van der Spuy and De Jongh Inc and Others* 2020 (1) SA 560 (GP). These cases can also provide useful training material for staff on business email compromise scams. Other cases that you can include in your training material are *Galactic Auto (Pty) Ltd v Venter* (4052/2017) [2019] ZALMPPHC 27 (14 June 2019) and *Lochner v Schaefer Incorporated and Others* (3518/16) [2017] ZAECPEHC 4 (24 January 2017). The *Hawarden v Edward Nathan Sonnenbergs Inc* and *Galactic Auto (Pty) Ltd v Venter* judgments differ from the other cases in a number of respects, including that in these two cases it was the party to whom payment was due to be made who

## RISK MANAGEMENT COLUMN continued...

was found liable whereas in the other cases it was the party making the payment who was found to be liable for making payment into an incorrect account.

Rule 54.13 of the rules issued in terms of the Legal Practice Act 28 of 2014 reads as follows:

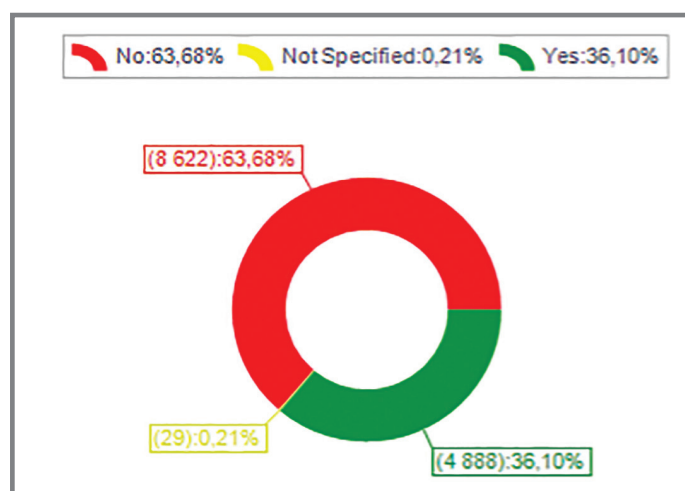
### “Payment to clients

54.13 A firm shall, unless otherwise instructed, pay any amount due to a client within a reasonable time. Prior to making any such payment the firm shall take adequate steps to verify the bank account details provided to it by the client for the payment of amounts due. Any subsequent changes to the bank account details must similarly be verified.”

Though rule 54.13 refers to payments to clients, the verification of the banking details and any subsequent or purported change must be applied to all payments.

The responses provided to the cybercrime related questions of the risk management self- assessment form make for interesting reading. The responses are as set out below. 97,78% of respondents indicated that they are aware of the risks associated with cybercrime. It is concerning that even with this claim of widespread awareness of this risk, the prevalence of firms falling victim to cybercrime is so widespread.

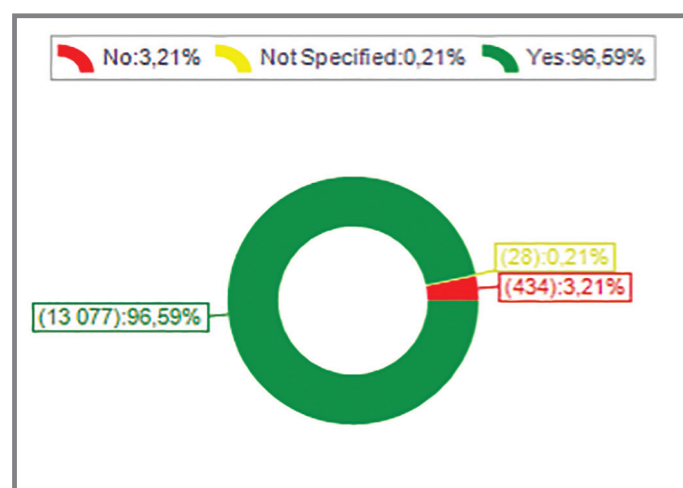
### Does your practice have appropriate insurance cover in place to cover cyber related claims?



The fact that just more than a third of legal practices indicate that they have appropriate cyber insurance in place is concerning as this risk is constantly increasing. Almost 97% of the respondents have stated that they conduct a verification of banking details as required by rule 54.13,

but the number of cyber related claims reported to the LPIIF and insurers in the commercial market paint a picture of a much lower percentage of firms with a verification system in place.

### In respect of the financial functions, has an adequate system been implemented which addresses the verification of the payee banking details, and any purported changes as required by rule 54.13?



In the wake of the recent judgments of law firms for cyber liability, legal practitioners must pay even more attention to this risk. There are a number of important lessons to be learnt from the judgments including raising awareness with all parties of the prevalence of cybercrime and business email compromise risks, including this risk in the training and orientation of staff, the implementation of secure portals and applications for communication (especially of banking details) and implementing a multi-factor authentication process.

### Conclusion

The claim statistics and some of the underlying information received when assessing and investigating claims contradicts the picture painted by the responses to the risk questionnaire. This is a serious concern in that the development and profile of risks cannot be accurately assessed if inaccurate information is provided.

LPIIF team is available to conduct risk management training for all legal practitioners and their staff. Please send an email to [risk.queries@lpiif.co.za](mailto:risk.queries@lpiif.co.za) should you require such training. The training is provided at no cost to legal practitioners and can either be done virtually or physically, depending on the needs of the firm.