REPUBLIC OF SOUTH AFRICA

IN THE HIGH COURT OF SOUTH AFRICA

GAUTENG DIVISION, PRETORIA

CASE NO: 2024/030523

(1) REPORTABLE: YES/NO
(2) OF INTEREST TO OTHER JUDGES: YES/NO
(3) REVISED.

..... **.....**
SIGNATURE **DATE**

In the matter between:

DIRKIE CORNELIA WESSELS Applicant

and

CAPITEC BANK LIMITED First Respondent

ABSA BANK LIMITED Second Respondent

ROWEN BRENT PETRUS Third Respondent

JUDGMENT

LABUSCHAGNE AJ

[1] The applicant is a 67-year-old pensioner who was scammed by fraudsters who obtained control over her bank account and paid an amount of R960 960.19 in 23 different transactions on the same day into bank accounts of the third respondent at Capitec Bank and Absa Bank.

[2] The two banks placed a precautionary hold on the accounts of the third respondent, but advised the applicant that they could not do so indefinitely. Unless they were provided with a court order extending the hold, they would release the hold on the accounts, thereby enabling the third respondent to continue transacting on his bank accounts.

[3] In Part A proceedings the applicant seeks urgent relief restraining the two banks from releasing the current hold on the third respondent's bank accounts pending finalisation of the determination of relief sought in Part B. The relief sought in Part B is repayment of the total of the deposits by the third respondent (R934 115) in an action envisaged to be instituted, as part of the Part A proceedings, within ten days of the granting of the court order. The applicant also seeks costs against any respondent opposing the relief in Part A.

[4] Only the third respondent has opposed the relief. He is a part time cryptocurrency trader on the Binance platform.

THE FACTS

[5] During 2023 the applicant received an inheritance from the proceeds of a sale of farmland which she invested in a six-month fixed account with Capitec Bank.

[6] On 2 February 2024 she received an SMS from an unknown person, stating: *"Payment notification: Transaction debited R11 700 on Takealot Ref-TXN77842. Not you or report call on 011 083 6652."*

[7] She was alarmed by the message as she had not ordered anything from Takealot. She called the number in the SMS and the call was answered by a certain "Tessa Smit" speaking with an Indian accent. She advised that she was working with Capitec's Fraud Department and that her investment account was hacked and that they suspect that it was an inside job.

[8] The applicant was instructed to go to a Capitec branch and to arrange for a transfer of her funds from her fixed account to a savings account. The applicant was assured by the fraudster that she was being helped to secure her funds from people who were trying to transact on her account and who were attempting to misappropriate her invested funds.

[9] She was instructed to go to a Capitec branch for a transfer into her savings account. She was assured that the costs of moving the funds between the accounts would be reimbursed by Capitec Bank.

[10] The applicant was requested to advise “Tessa Smit” via WhatsApp once the transaction was done in order for her to commence reversals of the transactions on her account.

[11] The applicant went to the Centurion branch of Capitec and transferred an amount of R1 026 590.23 into her savings account. She then advised “Tessa” that it had been done. The latter explained the process of rectifying and reversing the fraud. In order to do so the applicant was requested to permit the installation of an app called “AnyDesk” on her cell phone, which was then installed. From there the fraudsters took control of her phone and she was unable to perform any functions on the device. Soon afterwards she saw an amount of R3 500.00 being deposited into an Absa account in the name of Tarryn Hill. The applicant asked “Tessa” who this person was, and she said it is the account the hacker had paid her money into. She contended that she was busy reversing the transaction in order that it be returned to her account.

[12] Then the name of the third respondent appeared on her screen and also an Absa account. After this, more transactions were done to the third respondent, as his name kept appearing on the notifications on her screen. The applicant was advised by the fraudster that these transactions were happening on her account, but she was busy with the “Nigerian Fraud Department”. The telephone conversation lasted a few hours, and once she hung up, a notification came up on the applicant’s phone which showed that she only had R35.00 left in her account. It was at that stage that she realised that she had been scammed. She rushed to the Capitec branch to

obtain assistance, and her savings account was immediately frozen, and the matter reported to the Bank's Forensic Investigations Department. The applicant was also advised to lay a criminal charge at Lyttleton Police Station, which she did under CAS40/02/2024, making an affidavit to the Police.

[13] The transactions that took place on her account on 2 February 2024 demonstrate 23 transfers to the third respondent in the following batches:

13.1 R44 000.00;

13.2 R26 500.00;

13.3 R41 000.00;

13.4 R43 500.00;

13.5 R26 500.00;

13.6 R44 600.00;

13.7 R44 700.00;

13.8 R44 800.00;

13.9 R44 900.00;

13.10 R32 700.00;

13.11 R44 992.00;

13.12 R44 987.00;

13.13 R40 501.00;

13.14 R44 717.00;

13.15 R44 919.00;

13.16 R44 999.00;

13.17 R44 888.00;

13.18 R44 777.00;

13.19 R44 666.00;

13.20 R44 555.00;

13.21 R44 925.00;

13.22 R43 989.00;

13.23 R18 000.00.

[14] Absa Bank was informed by Capitec that the proceeds of fraudulent crime were transferred into accounts of their clients. The applicant was informed that the third respondent holds a bank account with Absa, being account number 4107120565.

[15] Every one of the withdrawals from the applicant's Capitec account were transferred directly into the third respondent's Capitec account. This is confirmed by an affidavit of Carolina Petronelle Botha, an employee of Capitec Bank made in terms of section 236 of the Criminal Procedure Act. In the affidavit she states that she examined the entries in the accounting records and documents of the bank and that it correctly sets out the attached copies of the third respondent's banks statements. They correlate with the withdrawals from the applicant's Capitec bank account.

[16] The third respondent's bank statements reflect that the opening balance on that day was in the region of R3 000.00. The transfers from the applicant's bank account then poured in. On the day in question, he transferred R26 500.00 and a further R29 500.00 from his Capitec account to his Absa account with the reference "Rowan Absa". These transfers were made from

the third respondent's Capitec account into his Absa account immediately after the funds of the applicant were transferred into his Capitec account.

[17] On 5 March 2024 the applicant was advised by Jannie Coetsee, a Manager at Capitec Forensic Investigation Department that they had managed to trace and recover certain of the amounts and transactions debited against her Capitec savings account. The recovered amounts were deposited into her savings account on 28 and 29 February 2024. The total amount so recovered was R467 125.70.

[18] The applicant was further advised that the third respondent held a savings account with Capitec Bank with account number 1450278599 in which there is a balance of R102 879.11. Capitec had placed a precautionary security hold on the account.

[19] The applicant was however advised by Mr Coetsee that, unless a court order was provided within a few days, the hold on the bank accounts would be released.

[20] The applicant's attempts to have the matter heard urgently faltered twice. In the first case it was struck from the roll when her counsel failed to appear on 12 March 2024. That application was withdrawn, and the current application was launched. However, the application was set down on a Wednesday, 3 April 2024, in the urgent court when it should have been set down for Tuesday, 2 April 2024. The court in the urgent judge declined to hear the matter due to the improper enrolment. The enrolment was caused by

counsel for the applicant having prior engagements on 2 April 2024 in Cape Town.

[21] This is therefore the third occasion on which the matter serves before court. The respondent contends that the applicant is abusing the court process and should be mulcted in special costs.

[22] The applicant intends instituting action proceedings against the third respondent. In her founding papers she contends that she intends instituting a *condictio furtiva*. The applicant contends that the third respondent received the funds *mala* fide.

[23] The third respondent is insisting that the banks release the hold, contending that the proceeds are his money, which he intends utilising as he deems fit.

[24] I am satisfied that the application is urgent and that, unless the urgent court were approached, the applicant would not obtain substantial redress in due course.

[25] As the interdict which the applicant seeks is anti-dissipatory, it is a requirement to establish that the third respondent has the intention of dissipating the assets with the intention of defeating the applicant's claim.

[26] In **Poolman v Cordier and Others** [2017] ZANCHC 49 (at par [17]) Erasmus AJ said:

"[17] A Mareva injunction is a species of an interim interdict compelling a respondent/defendant to refrain from dealing freely with his assets to which the applicant can lay no claim. The purpose thereof is to prevent the intended defendant, who can be shown to have assets and who is about to defeat the plaintiff's claim by dissipating assets, from doing so. To be successful, the applicant must show that the respondent is wasting or secreting assets with the intention of defeating the claims of creditors."

[27] In **Polly Peck International Plc v Nadir and Others (No. 2)** [1992] 4 All E.R. 769 (CA) 785 G – H the Court of Appeal said:

"It is not the purpose of a Mareva injunction to prevent a defendant acting as he would have acted in the absence of a claim against him." (See also **Evoke Reality (Pty) Ltd v Jacobus and Others** 2023 (JDR) 3221 (GJ), para [34] to [35]).

[28] It is therefore necessary to enquiry into whether the applicant has established *mala fides* in the aforesaid sense.

[29] The third respondent has admitted all the transactions are from the transferring of funds from the applicant's account into the accounts of the third respondent. It is common cause that the applicant was a victim of fraud and/or theft.

[30] The third respondent is a cryptocurrency trader (albeit part time).

[31] The third respondent contends that there was nothing sinister in the large volume of cryptocurrency purchased. He contends that he is an unsuspecting *bona fide* third party.

[32] The applicant contends that the third respondent is not as *bona fide* as he professes to be.

[33] The applicant contends that the third respondent failed to verify the identity of his client and failed to verify the source of funding. These obligations, so argues the applicant, are imposed by law.

[34] Furthermore, the pattern of transactions emanating from the same client in a very short period of time under the threshold of R45 000.00 should have raised red flags, thereby prompting the third respondent to make enquiries.

[35] The third respondent disputes that the applicant can establish that he intends dissipating assets with the purpose of frustrating her claim. The applicant, for example, does not allege that the third respondent is the scamster. He contends that she has a claim against the scamsters and not against him.

[36] The third respondent contends that the applicant has willingly (and blindly so) allowed and facilitated vast sums of money to be paid from her bank account to third parties and communicated with scamsters to release the funds. He contends that she should have known that she was being scammed, as she admitted in retrospect.

[37] The third respondent contends that, unbeknown to him, the scamsters utilised the applicant's stolen funds to purchase cryptocurrency from the third respondent. Once purchased, the cryptocurrency was transferred by the third respondent to the "designated wallet", i.e. the account held by scamsters (but unbeknown to the third respondent). The third respondent therefore contends that he sold his cryptocurrency as part of a legitimate business activity, transferring value in receipt for the purchase price.

[38] The applicant fails to allege and substantiate that the third respondent is dealing with his assets with the intention of defeating her claim.

[39] The third respondent contends that the bank accounts in question are his daily transactional accounts. He runs his part time business through those accounts. His salary is paid from the Capitec account number 1450278599 as are his living expenses. He pays from his Capitec account into his Woolworths credit card, from which he pays his accounts. He contends that he will be unable to do so if the hold on the accounts is not uplifted and he is not enabled to access the funds to pay for ordinary living expenses, including food and the like.

[40] The respondent contends that, as a result of *commixtio*, the applicant is unable to obtain an order preserving *"her funds"*.

[41] The respondent then set out his activities as a cryptocurrency trader. He has traded with more than 268 parties and has facilitated more than 682

trades. He has sold cryptocurrency on 498 occasions and in 184 occasions he has purchased cryptocurrency.

[42] The respondent trades via a company known as Binance, which is an international company that operates the largest cryptocurrency exchange platform in the world. There are more than 350 different cryptocurrencies available for trading purposes. It provides a platform for users to buy, sell and trade a variety of cryptocurrencies.

[43] The third respondent's Binance nickname is "Pierty". He primarily trades on Binance through the buying and selling of Tether Dollars. Tether is an asset backed cryptocurrency stablecoin. Tether are digital tokens that represent a claim on the underlying reserve of a fiat currency – US Dollar.

[44] The respondent buys cryptocurrency and advertises it for sale in an advertisement that he posts on Binance's P2P trading platform or exchange ("Binance P2P").

[45]

45.1 If a purchaser were interested in the advertised transaction, the purchaser would click on the advertisement and place an order. The Tether Dollars are tradable and are transferred to the purchaser via the platform.

45.2 As soon as a purchaser agrees to place an order, the currency they intend to purchase is held in Trust or security by Binance. Binance acts as an intermediary and the buyer has 15 minutes to make

payment for the specific purchase into the third respondent's bank account.

45.3 Should the buyer make payment within the 15 minutes, the buyer returns to the trading platform and marks the order as paid. The respondent in turn logs into his bank account to confirm that the money is reflected there, that it matches the amount in Binance and that the reference number for the payment is the same for the bank and Binance payments.

45.4 The sale is completed when the third respondent goes to Binance to confirm that he has received the correct deposit. Once the process has been completed, Binance releases the cryptocurrency that it holds in Trust or security to the buyer's designated cryptocurrency wallet, i.e. the buyer receives the cryptocurrency that it purchased from the third respondent, and he receives the funds in turn.

[46] The third respondent trusted Binance to verify the identity of the purchaser. The respondent contends that all the requirements in terms of FICA were complied with by the very nature of registering and doing business on Binance. He states: *"It is one of the reasons that I trade with Binance as it assures that all the FICA requirements are met as all users of Binance identities are verified and copies of their IDs taken."*

[47] The evidence establishes that the scamsters put the applicant through all the steps required to register her identity on Binance without her knowing that

she was doing so. This included a photograph taken with movement of the head.

[48] The facts of this matter indicate that the Binance platform assists in identifying persons who are being defrauded in money laundering schemes but does not identify the fraudsters who are transacting on the Binance platform on behalf of such victims.

[49] The third respondent's acceptance that Binance had complied with all the FICA requirements loses sight thereof that the Binance platform can itself be utilised by fraudsters to register their victims as clients, whilst the fraudsters transact anonymously on the Binance platform on their accounts.

CRYPTOCURRENCY TRADERS AND FICA

[50] The Financial Intelligence Centre Act defines "accountable institution" as a person referred to in Schedule 1. Item 22 of the Schedule 1 refers to cryptocurrency traders and states the following:

"A person who carries on the business of one or more of the following activities or operations for or on behalf of a client:

(a) exchange of crypto asset for a fiat currency or vice versa;

(b) exchanging one form of crypto asset for another;

(c) conducting a transaction that transfers a crypto asset from one crypt asset address or account to another;

(d) Safeguarding or administration of a crypt asset or an instrument enabling control over a crypto asset; and

(e) Participation in and provision of financial services related to an issuer's offer or sale of a crypto asset,

where 'crypto asset' means a digital representation of perceived value that can be traded or transferred electronically within a community of users of the internet who consider it as a medium of exchange, unit of account or store of value and use it for payment or investment purposes, but does not include a digital representation of a fiat currency or a security as defined in the Financial Markets Act, 2012."

[51] The obligations imposed on an accountable institution in terms of FICA include the obligation to develop, document, maintain and implement a programme for anti-money laundering (section 42(1) of the FICA). The Risk Management and Compliance Programme (RMCP) must enable the accountable institution to identify, assess, monitor, mitigate and manage the risk that the provision by the accountable institution of new and existing products or services may involve or facilitate money laundering activities (section 43(2)(a) of the FICA).

[52] The aforesaid RMCP must provide for the manner in which the Institution determines if a person is a prospective client, in the process of establishing a business or entering into a single transaction with the institution- or is a client who has established a business relationship or entered into a single transaction (section 42(2)(b)).

[53] More in point, section 42(2)(d) requires such RMCP to provide for the manner in which, and the processes by which the establishment and verification of the identity of persons, whom the accountable institution must identify in terms of Part 1 of the FICA Chapter, is performed in the institution.

[54] Part 1 is a reference to the due diligence provisions in FICA, which provide *inter alia* for the identification of clients (section 21), the duty to keep record pertaining to a client or prospective client (section 22 and section 22A) and keeping of records for the prescribed five-year period from date of termination of the business relationship (section 23(a)).

[55]

55.1 When an accountable institution engages with a prospective client to enter into a single transaction or to establish a business relationship, the accountable institution must establish and verify the identity of the client.

55.2 If the client is acting on behalf of another person, the accountable institution must establish and verify the identity of that other person and verify the client's authority to establish the business relationship on behalf of that other person (section 21(1)(a) to (c)).

[56] An accountable institution must report transactions to the Financial Intelligence Centre with a client if, in terms of the transaction, an amount of cash in excess of the prescribed amount (R49 999.00) is received by the

accountable institution from the client, or from a person on behalf of the client, or from a person on whose behalf the client is acting (section 28(4), read with Regulation 22B of the Money Laundering and Terrorist Financing Control Regulations GNR1595 in GG24176 of 20 December 2002).

[57] The duty to report transactions is not limited to transactions in excess of the threshold. There is also a duty in terms of FICA to report suspicious or unusual activities (sec 29).

[58] The third respondent received an order to purchase cryptocurrency for R33 000.00 on 2 February 2024 from a person reflected on the Binance platform as being the applicant. This was the first time such an order was received. After this first transaction, the “applicant” continued to purchase large volumes of currency. The third respondent says that there was nothing sinister in this large volume, because he had reduced the price of the cryptocurrency that he had advertised. The “applicant” requested the third respondent to restock his currency to facilitate the purchasers. Due to the volume being purchased, the applicant reached the cap of R100 000.00 from and to external banks. The applicant then requested the third respondent to use his Capitec Bank account, i.e. a different bank account which he then did.

[59] Twenty-three transactions later, the orders and payments via the Binance platform totalled R934 115.00

[60] Throughout this process the third respondent was unquestioning. The fact that such a multitude of transactions came through under the limit of R50 000.00 was in itself a red flag which obligated the third respondent to report the transactions to FICA as being suspicious. His failure to verify the identity of his true client in respect of the trades is the reason why these transactions proceeded at all.

[61] The third respondent as cryptocurrency trader cannot delegate his obligations to identify his client as required by FICA to Binance. That platform cannot verify that the registered client is in fact the person transacting on the Binance platform.

[62] The third respondent is ostensibly washing hands of his obligations in terms of FICA and, in fact, blames the applicant for being scammed.

[63] A cryptocurrency trader in the position of the third respondent should foresee the risk of money laundering on a platform like Binance and for that reason verify the identity of his clients. The risk of harm is there for all to see. He is ostensibly indifferent to the consequences of his failure to comply with his statutory duties to the public who trade on the platform with him as cryptocurrency trader. Such indifference is lamentable.

[64] Despite the aforesaid, the mere presence of *mala fides* in receiving the funds by virtue of such indifference and in breach of statutory duties, is not enough to establish the risk that the third respondent intends dissipating assets with the view to frustrating the claim of the applicant.

[65] In the absence of an allegation to this effect and evidence in support thereof, the applicant can therefore not establish a *prima facie* right for the interdict sought.

[66] In the light of the aforesaid finding, it is not necessary to traverse the remainder of the requirements for an interim interdict.

[67] A trader in the position of the third respondent has duties to the public in terms of FICA to prevent money laundering. In an appropriate case, such a trader may be held liable in delict. It is not necessary for me to make any pronouncements in this regard in this matter.

[68] Despite the application failing by virtue of the aforesaid, the third respondent has clearly failed the applicant. His failure to verify her identity and his indifference to her loss in these circumstances is the reason why I make the cost order below:

1. The application is dismissed.

2. No order as to costs.

LABUSCHAGNE AJ

ACTING JUDGE OF THE HIGH COURT

Appearances

For the applicant	Lily Rautenbach pta@lilyrautenbach.com
Instructed by	Lily Rautenbach Attorneys Adv G Kasselman Circle Chambers
For the third respondent	Mr M Schrueder shaheid@schrueder.co.za Schrueder Incorporate Attorneys c/o Hurter Spies Attorneys Adv N Terblanche