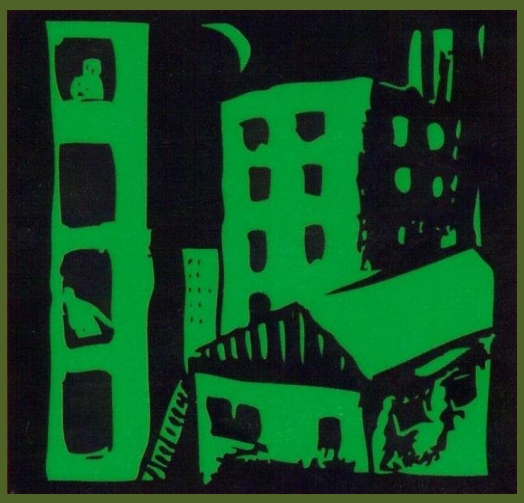
LAW
DEMOCRACY
& DEVELOPMENT



VOLUME 17 (2013)

DOI: http://dx.doi.org/10.4314/ldd.v17i1.3

ISSN: 2077-4907

Phishing in the world wide web ocean: *Roestof v Cliffe Dekker Hofmeyr Inc* – A case of cyber laundering through an attorney's trust account

ABRAHAM HAMMAN*

Lecturer, Faculty of Law, University of the Western Cape

1 INTRODUCTION

Money launderers are always exploring new channels to clean their ill-gotten gains. The attorney's trust account is especially attractive to persons, or organisations, that seek to launder money.[1] As a result, the Financial Action

* I am grateful to Professor Solly Leeman for his comments on the earlier drafts of this article and to Adrian Hamman who came up with the title of this article.

[1] Shepherd K "USA Patriot Act Surprising implications for transactional lawyers" (2002) *Probate & Property* 26. LAWPRO 2003 "Respecting the 'Trust' in Trust account" at www.practicepro.ca/LAWPROMag/march2003_trusts.pdf (accessed 20 March 2013).

Task Force (FATF) has included lawyers amongst other professionals who are regarded as targets in complex money laundering schemes.[2] In *Roestof v Cliffe Dekker*[3] (Roestof) a trust account of an attorney was transformed into an instrument of crime and manipulated in pursuit of a criminal purpose.[4] This crime was in the process hidden behind the veil of credibility which attaches to the trust account.[5] Attorneys' firms have vast amounts of money in their trust accounts. They must be heedful, on the one hand, of not becoming victims of money launderers as a result of phishing schemes and, on the other hand, they must be alert to the fact that their accounts may be used as one-stop laundromats to clean the money.[6] In this article the behaviour of two attorneys will be discussed: the one attorney, Roestof, whose money was fraudulently transferred out of his Absa Bank private account, and Adriaans, the other, a director at the time of Cliffe Dekker, who caused the money to be transferred to the cyber launderer. The article then further examines the court's failure to discuss the conduct of the attorneys in relation to suspicious and unusual transactions and includes recommendations as to how attorneys can put safeguards in place to avoid becoming victims.

In *Roestof,*[7] an amount of R350 000 was fraudulently transferred out of the plaintiff's personal account, and R200 000 thereof was cleaned via the trust account of the defendant firm. One of the directors of the firm was led to believe that the firm was receiving payment of a debt due to one of its clients. It was the client who used the attorney firm's trust account as a conduit to decontaminate the criminal proceeds of the phishing scam and caused the onward transmission of the money to another party. Attorneys need to be much more watchful to avoid becoming victims of phishing schemes and be much more alert to the fact that there are criminals who may masquerade as clients, who will utilise their accounts as devices to clean their ill-gotten gains.

2 CYBER LAUNDERING

The internet is a global network of computers that is able to transmit and receive information with the touch of a few keys on a computer, and has become an essential part of our daily lives.[8] Furthermore, the internet expansion has made it possible to

---

[2] Report on money laundering typologies 2000-2001, FATF 14. It should be noted that recommendations made by FATF in February 2012 have not been incorporated into the Financial Intelligence Centre Act 38 of 2001. Specifically, Recommendation 10 from FATF strengthens the requirements for banks on behalf of customers in situations similar to this in Roestof. Recommendation 17 further enhances those protections which, had they been in place, might have assisted in the resolution of the matter in Roestof.

[3] *Roestof v Cliffe Dekker Hofmeyr Inc* (34306/2010) [2011] ZAGPPHC 219 (2012).

[4] Hamman and Koen "Cave Pecuniam: Lawyers as Launderers" (2012) 15 *PELJ* at 69.

[5] Hamman and Koen (2012) at 69.

[6] Hamman and Koen (2012) at 69.

[7] See *Roestof v Cliffe Dekker Hofmeyr Inc* para 2.

[8] Richards J *Transnational Criminal Organizations, Cybercrime, and Money Laundering* (1999) at 69.

Van Jaarsveld "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" (2004) *SA Merc LJ* at 694; Ping "New Trends in Money Laundering -From the Real World to Cyberspace" (2004) *JMLC* at 50; Phillipsohn "The Dangers of New Technology- Laundering on the Internet" (2001) *JMLC* at 87.

transfer money almost immediately through cyberspace.[9] The movement of money via the internet has become very effective and enables individuals to execute their financial transactions on-line, thereby making visits to a bank almost unnecessary.[10] The modern monetary system consists of digital money transfers or electronic funds transfers (EFTs) through telecommunication links among bank computers.[11] Internationally, banks are linked by a computer messaging system that is operated by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)[12]. Domestic banks within a country use systems similar to the Clearing House Interbank Payment System (CHIPS).[13] It is these systems that enable private individuals and companies to conduct their business through the internet.[14]

Law offices also utilise this technology to transfer their clients' money by electronic means. This regularly occurs in conveyancing and commercial transactions. Regrettably this has also provided money launderers with an opportunity to perpetrate crime via the trust accounts of legal practitioners. Criminals, who are able to access someone else's funds, exploit this form of technology as a kind of anonymous banking and if successful, their schemes allow them access to an infinite source of almost untraceable wealth.[15] Cyber laundering is ideal from a launderer's point of view, because of the potential anonymity and that the financial crimes committed in cyberspace are almost undetectable. The Internet allows people to hide themselves among millions of other users, pretending to be someone else since it is difficult to be identified.[16] This was discovered by Roestof who became a victim of such a crime when he divulged confidential information after responding to a phishing scam.

3 THE PHISHING SCAM

Phishing is a technique employed by identity thieves to acquire personal information, such as, the names, account numbers, passwords, identity numbers and credit card details of users, by using deceptive e-mail messages that appear to originate from legitimate businesses.[17] The term "phishing"[18] originates from the way that the fraudster uses e-mails as bait, similarly to a fisherman, to fish for profitable personal

[9] Weatherford J *The History of Money* (1997) at 248. "Throughout its history, money has become steadily more abstract. By moving at the speed of light, electronic money has become the most powerful financial, political and social force in the world. Money has become even more like God: totally abstract and without corporeal body."

[10] Richards (1999) at 69, Phillipsohn (2001) at 87.

[11] Ping (2004) at 49, Joyce "E-diligence: money laundering risks in the electronic arena" (2001) *JMLC* at 146.

[12] Ping (2004) at 49, Madinger J *Money Laundering: A Guide for Criminal Investigators* (2012) 175-176.

[13]Ping (2004) at 49, Madinger (2012) at 175-176.

[14] Ping (2004) at 51, Joyce (2001) at 146, Richards (1999) at 69.

[15] Van Jaarsveld (2004) at 685.

[16] Filipkowski "Cyber Laundering: An Analysis of Typology and Techniques" (2008) *IJCJS* at 15.

Armstrong and Forde, "Internet anonymity practices in computer crime", (2003) *IMCS* at 209 – 215.

[17] Fox "Phishing, pharming and identity theft in the banking industry" (2006) JIBLR at 548.

[18] AlMahroos "Phishing for the answer: recent developments in combating phishing" (2007) *JLPIS* at 595.

information from unsuspecting internet users.[19]

In *Roestof*, the scheme operated as follows. On 14 January 2010, Roestof received an e-mail that seemed to originate from Absa Bank (Absa).[20] In the e-mail the client is warned that Absa suspected that fraudsters are attempting to gain access to his account.[21] He was then requested to click on a link shown in the e-mail and because he had had difficulty accessing his internet banking account the previous day, he clicked on the link.[22] This led him to what he thought was the first page of the Absa internet banking service, he entered his login details and then clicked "next". After he received a sms[23] from what he thought was an Absa number, he clicked onto the second Absa page.

Absa has a unique safety feature, called a "surephrase", which is given to an internet client making use of accounts via the internet for the first time.[24] The client is requested to select his own "surephrase" and every time that he logs on thereafter this "surephrase" is shown.[25] This device is an indication that the site is protected and that the client can continue with the transaction. Roestof, when he testified, could not say whether he saw his "surephrase" on the webpage; in fact, he was unaware of the existence of the "surephrase".[26] During the trial he was requested by the court to go onto the Absa website to verify that the "surephrase" indeed appeared on his screen, which he did, and he confirmed this later in court.[27]

After accessing the second internet page, he then entered his password and received another sms requesting him to confirm it, which he did.[28] It is unclear whether he just left the page or performed any other transactions that day. It must be accepted that he then left the internet banking site. The scam was that a bogus website had been created by the cyber launderer and that when Roestof entered his account particulars that information was intercepted and used by the launderer to access the account.

About two hours after he left the website, at about 19:00, Roestof received a message to call Michelle at Absa's fraud department.[29] He contacted the fraud department and spoke to Sabela, who informed him that an amount of money had been fraudulently withdrawn from his account. He was not informed what the amount was

[19] *Roestof v Cliffe Dekker Hofmeyr Inc* para 4.
[20] *Roestof v Cliffe Dekker Hofmeyr Inc* paras 2 and 24.
[21] *Roestof v Cliffe Dekker Hofmeyr Inc* para 24.
[22] *Roestof v Cliffe Dekker Hofmeyr Inc* para 24.
[23] Short Message Service, a type of automatic text message service often used to provide an instant communication or notification to a subscriber's cell phone.
[24] Phishing Scams http://www.absa.co.za/Absacoza/Security-Centre/Online-Security/Absa-Online-Security-Measures (accessed 20 March 2013).
[25] Phishing Scams http://www.absa.co.za/Absacoza/Security-Centre/Online-Security/Absa-Online-Security-Measures (accessed 20 March 2013). *Roestof* para 8.
[26] *Roestof v Cliffe Dekker Hofmeyr Inc* para 26.
[27] *Roestof v Cliffe Dekker Hofmeyr Inc* para 26. See http://www.absa.co.za/Absacoza/Security-Centre/Online-Security/Absa-Online-Security-Measures (accessed 20 March 2013).
[28] *Roestof v Cliffe Dekker Hofmeyr Inc* para 27.
[29] *Roestof v Cliffe Dekker Hofmeyr Inc* para 28.

and into whose account the deposit was made. Since it was already after banking hours, he decided to go to the bank and the police the following day.[30]

4 THE MANIPULATION OF DEFENDANT'S TRUST ACCOUNT

About two months prior to the phishing incident, mentioned above, on 20 November 2009, Adriaans, a director at the time of the defendants firm, received telephonic instructions from a Peter Slinger to collect R1 million from one of his company's debtors.[31] Slinger stated that he acted on behalf of an entity, Sewmach Sewing Machines (Sewmach). The instructions were that the debtor was a company named Newbucs Ops Trading Bk (Newbucs). Adriaans never met Slinger in person and requested him to send the necessary supporting documentation to the firm to enable it to open a file.[32]

A pack of documents was sent to Adriaans, and although Slinger was referred to as a managing director of a close corporation,[33] Adriaans did not find it to be out of the ordinary. It must be noted that the parties in a close corporation are referred to as members and not directors.[34]

During cross-examination in court, Adriaans however admitted that he had not read the documentation and that the number of documents that he had received for purposes of verification in terms of the Financial Intelligence Centre Act[35] (FICA), were forwarded to the FICA officer of the firm.[36] It must be accepted that the FICA officer found the documentation to be acceptable for verification of the identity of the members of the close corporation.[37]

According to the evidence presented in court, all the correspondence in this matter was sent via e-mail and the client did not visit the offices of the firm at any stage during this period.[38] A few days after the initial instructions were given to Adriaans, a Charles David on behalf of Sewmach sent an e-mail to him that Newbuc's foreign partner had contacted Sewmach and made arrangements to settle the amount owing to it.[39] David advised that because Sewmach had already instructed the defendant to collect the money, it preferred that the money owed be paid into the defendant's trust account. After David requested the banking details of the defendants, Adriaans forwarded the details of its Standard Bank account to Newbucs.

There was no communication between Sewmach and Adriaans between November 2009 and January 2010. On 14 January 2010, David again got in touch with

[30] *Roestof v Cliffe Dekker Hofmeyr Inc* para 28-30.
[31] *Roestof v Cliffe Dekker Hofmeyr Inc* para 16.
[32] *Roestof v Cliffe Dekker Hofmeyr Inc* para 16.
[33] *Roestof v Cliffe Dekker Hofmeyr Inc* para 17. Ss 28 and 29 Close Corporation Act 69 of 1984.
[34] Ss 28 and 29 Close Corporation Act 69 of 1984.
[35] The Financial Intelligence Centre Act 38 of 2001.
[36] *Roestof v Cliffe Dekker Hofmeyr Inc* para 18.
[37] *Roestof v Cliffe Dekker Hofmeyr Inc* para 86.
[38] *Roestof v Cliffe Dekker Hofmeyr Inc* para 15.
[39] *Roestof v Cliffe Dekker Hofmeyr Inc* para 19.

Adriaans via e-mail.[40] David informed him that Newbucs had made arrangements to deposit the amount of R200 000 into the Standard Bank trust account of the defendant. There was no explanation given as to whether the claim of R1 million was now being settled with the amount of R200 000. Attached to David's e-mail was an e-mail from Newbucs confirming that the deposit had been made into the defendant's account. The e-mail from Newbucs read: "Our company accounts department have made the payment of R200 00,00 to your attorneys Standard Bank account today. The payment reference used services charges as usual."[41]

In his e-mail David informed Adriaans that Sewmach required the money without delay and requested him to pay the amount into the Nedbank account of M J Slingers t/a Sewmach as soon as possible.[42]Nothing was mentioned about the balance owed to Sewmach.

5 EVENTS AFTER 14 JANUARY 2010

On Friday 15 January 2010, Roestof went to his private banker, a Van der Merwe, who told him that an amount of R350 000 had been transferred out of his account; and that R200 000 of this had been transferred to a Standard Bank account number.[43] He was handed a statement confirming the amount withdrawn from his account.[44] Van der Merwe gave the account number to him, but not the account holder's name. On the same day Roestof also laid a complaint with the police. What is odd is that there was no evidence why Roestof did not insist on getting the particulars of the Standard Bank account. Surely, as an attorney he must have been aware that if he obtained the particulars of the said account, he could approach the court on an urgent basis for appropriate relief to prevent the money being paid out to anyone.[45] There was no explanation as to why the plaintiff did not approach the court at that stage on the Friday to interdict the defendant from paying out the money.

On Monday 18 January 2010, subsequent to receiving confirmation that the deposit had been received, Adriaans debited a fee of R5831,60 and instructed the firm's accounts department to transfer the balance of R194 168,40 into the Nedbank account which David had given him.[46] As a result of David's request that the money be paid over urgently, Adriaans requested the accounts department that payment be made out of the firm's Nedbank trust account. The money was then duly transferred on 18 January 2010. On 19 January 2010, the fee of R 5831,60 was transferred from the trust account to the defendant's business account.[47]

---

[40] *Roestof v Cliffe Dekker Hofmeyr Inc* para 20.
[41] *Roestof v Cliffe Dekker Hofmeyr Inc* para 20.
[42] *Roestof v Cliffe Dekker Hofmeyr Inc* para 21.
[43] *Roestof v Cliffe Dekker Hofmeyr Inc* para 29.
[44] *Roestof v Cliffe Dekker Hofmeyr Inc* para 32.
[45] *Nissan SA Pty Ltd v Marnitz* 2005 (1) SA (SCA) 441 para 24.
[46] *Roestof v Cliffe Dekker Hofmeyr Inc* para 36.
[47] *Roestof v Cliffe Dekker Hofmeyr Inc* para 37.

On Wednesday 20 January 2010, Roestof, after being unable to obtain any assistance from Absa, approached his law firm's private banker, a Ramnath, at Standard Bank to assist him.[48] He was only informed on 25 January 2010 that the amount could only be frozen if he obtained a court order.[49] This seems to be strange advice, as the amount of R200 000 had already been paid out on 18 January 2010. Roestof only found out on 8 February 2010 that the R200 000 had been transferred to the defendant's trust account.[50] Plaintiff only instituted action against the defendant in June 2010. All three stages of the money laundering process, namely, the placement[51] (when the money was fraudulently withdrawn and then deposited in defendant's account), the layering[52] (when the mixing of the money with other trust monies occurred) and the integration[53] (when the money was transferred out of the trust account back into the financial system into the account of the launderer) took place within only a few days. It had all the features of a legitimate transaction where an attorney collected money on behalf of a client, deducted his fees and paid the balance to the client.[54]

6 THE JUDGMENT

Roestof's claim against the defendant failed for a number of reasons. The court, per *Du Plessis J,* held that the claim based on the *rei vindicatio* could not succeed, and also found that the defendant had not been enriched with the money in question.[55] The plaintiff's claim that the defendant paid out the money regardless of the fact that he had a right to the money also failed.[56] The court held that the defendant was unaware that the money had been fraudulently transferred to its trust account and that Adriaans only became aware thereof on 25 January 2010 when the money had already been paid out.

Roestof's argument that the defendant knew it was his money, was rejected by the court and it held that the defendant only became aware of this on 25 January 2010.[57]

---

[48] *Roestof v Cliffe Dekker Hofmeyr Inc* para 38.

[49] *Roestof v Cliffe Dekker Hofmeyr Inc* para 41.

[50] *Roestof v Cliffe Dekker Hofmeyr Inc* para 41.

[51] Placement is the stage at which the proceeds of an economic crime, usually bulk cash, are converted into a more portable and less suspicious form and injected into the financial system. Richards (1999) at 11. Madinger (2012) at 7.

[52] This stage focuses upon the creation of false paper trails by means of single or multitudinous transactions across several locations (accounts) and/or jurisdictions Hinterseer "An Economic Analysis of Money Laundering" (1997) 1:2 *Journal of Money Laundering* 154 at 155.

[53] This is the stage at which the laundered money, its links to illegality now sundered, is reintroduced into the mainstream economy. Hinterseer (1997) at 155.

67. Richards (1999) at 51.

[54] Ss 78 and 83(9) of the Attorney's Act 53 of 1979 and CLS Rule 20 http://www.capelawsoc.law.za/docs/CLS%20Rules%20Amended%20Oct%202011%20FINAL.pdf (accessed 20 March 2013); *Law Society, Transvaal v Matthews* 1989 (4) SA 389 (T); *Holmes v Law Society of the Cape of Good Hope and Another* 2006 (2) SA 139 (C); *Summerley v Law Society, Northern Provinces* 2006 (5) SA 613 SA; and *The Law Society of the Cape of Good Hope v Peter* [2006] SCA 37.

[55] *Roestof v Cliffe Dekker Hofmeyr Inc* para 57.

[56] *Roestof v Cliffe Dekker Hofmeyr Inc* para 45.

[57] *Roestof v Cliffe Dekker Hofmeyr Inc* para 68.

The court also held that defendant had no legal duty to find out or to determine whose money was deposited into its trust account.[58] The court held that Roestof never had a contractual relationship with the defendant as a client, and that it was not necessary for the defendant to obtain Roestof's instructions or consent to transfer the money out of its trust account.[59]

The court had to ascertain whether Roestof's claim that the defendant negligently and illegally failed to establish that the money came from him had any merit. The court dealt with an attorney's duty in terms of his trust account.[60] It held that attorneys from time to time receive deposits into their trust accounts without knowing the identity of the depositor; any such deposit must first be placed in a suspense account until the depositor has been identified.[61] Only once the depositor has been identified must a journal entry be made and the amount entered against the correct trust creditor.[62] In this case Adriaans was aware of his client's identity. He knew that he received instructions from Sewmach and that the payment into his trust account which was made by Newbucs was for the account of Sewmach. The defendant in fact received a deposit slip as proof of payment of the amount of R 200 000. The fact that the deposit was fraudulent was only discovered afterwards. Although Adriaans's handling of the transfer of the trust money and the payment of the fee could be criticised, the court found that Adriaans had made the necessary enquiries before he authorised the payment.[63]

The court also referred to *Hirschowitz Flionis v Bartlett,*[64] where money was fraudulently deposited into a trust account, and confirmed that the defendants had a duty to deal with the money without negligence.[65] This also applies to a person who is not a client of the attorney, as was the situation in the present case. The court stated that the lawyer's duty extended to the defendant and accepted that the defendant had a legal duty to the plaintiff to deal with the deposit in a way that would not cause damage to the plaintiff.[66] The court felt that the key question that it had to decide was whether the defendant had been negligent in dealing with the money deposited into its trust account.

The court established that there was no duty on a defendant to ascertain the origin of the money and, as previously indicated, that if an attorney was unable to verify the identity of the depositor, such amount must be kept in a suspense account until the

[58] *Roestof v Cliffe Dekker Hofmeyr Inc* para 69. *Du Preez v Zwiegers* 2008 (4) SA 627 SCA paras 19-21; *Hirschowitz*

Flionis v Bartlett 2006 (3) SA 575 (SCA) para 30.

[59] *Roestof v Cliffe Dekker Hofmeyr Inc* para 71.

[60] See discussion by Hamman and Koen (2012) at 69.

[61] *Roestof v Cliffe Dekker Hofmeyr Inc* para 76. *Hirschowitz Flionis v Bartlett* para 30.

[62] *Roestof v Cliffe Dekker Hofmeyr Inc* para 76.

[63] *Roestof v Cliffe Dekker Hofmeyr Inc* para 89.

[64] See *Hirschowitz Flionis v Bartlett* para 30.

[65] S 78 of Attorneys Act 53 of 1979.

[66] *Roestof v Cliffe Dekker Hofmeyr Inc* para 83. *Du Preez v Zwiegers* 2008 (4) SA 627 SCA paras 19 and 20.

identity of the depositor or of the client was determined.[67] The court emphasised however, that, before an attorney can deal with a deposit the identity of the depositor and for whose benefit (which client) the money was deposited have to be ascertained. In this case, the defendant established that the payment came from Newbucs, because David had informed Adriaans that the payment would come from them.[68] The court held that Adriaans was misled about the origin of the deposit, but that he thought that he was obliged to deal with the money in accordance with Sewmach's instructions. The question that the court had to decide was whether Adriaans could reasonably have foreseen or realised, that he was misled about the origin of the deposit.

The court found that Sewmach was a client who, in accordance with FICA obligations had been identified and evaluated by the defendant's staff who were authorised to do the FICA checking. There was no evidence that the person/department that did the FICA verification had any suspicion that something was amiss.[69] Before the deposit was made into the trust account, Adriaans was informed about the pending deposit and nothing at that stage prompted him to become suspicious.[70] After the payment was made into the trust account, Adriaans was furnished with the deposit slip as proof thereof. This also was not suspicious as it is common practice that clients send proof of payments to their attorneys by either e-mailing or faxing deposit slips. Although one could question Adriaans's conduct of not checking the reference on the deposit slip, the court held that he could not be expected to have come to the conclusion that the deposit was potentially fraudulent.[71] The court found that Adriaans had a reasonable belief that the deposit came from Newbucs; and that he had not been negligent.[72] The court found that Roestof was the author of his own dilemma as he did not read the warnings on the internet page of Absa, and that the fact that he could not recall whether there was a "surephrase" code on Absa's website confirmed that he had been negligent. Only after being requested by the court to verify if such a security phrase is available on the Absa website, did he go to check and confirmed it in court.[73] The court took this ignorance on the part of Roestof as confirmation of his negligence.[74]

The court rejected Roestof's testimony that he did not reveal his personal details during the phishing scam, and found that he indeed had disclosed his personal information when he entered his particulars on the duplicate website of the cyber launderer; and that it was the plaintiff's own negligence which contributed to his loss.[75]

[67] *Hirschowitz Flionis v Bartlett* para 30.
[68] *Roestof v Cliffe Dekker Hofmeyr Inc* para 85.
[69] *Roestof v Cliffe Dekker Hofmeyr Inc* para 86.
[70] *Roestof v Cliffe Dekker Hofmeyr Inc* para 87.
[71] *Roestof v Cliffe Dekker Hofmeyr Inc* para 91.
[72] *Roestof v Cliffe Dekker Hofmeyr Inc* para 92.
[73] *Roestof v Cliffe Dekker Hofmeyr Inc* para 26.
[74] *Roestof v Cliffe Dekker Hofmeyr Inc* para 93.
[75] *Roestof v Cliffe Dekker Hofmeyr Inc* para 93.

7 SUSPICIOUS AND UNUSUAL TRANSACTIONS IN TERMS OF FICA

Unfortunately, when the court dealt with the negligence of Adriaans, it failed to discuss the duty of practitioners in terms of section 29 of FICA.[76] This section stipulates how attorneys should act in response to suspicious and unusual transactions. The dangers of attorneys' trust accounts falling victim to the plotting of money launderers are addressed for the most part in section 29, which provide for mandatory suspicious transaction reporting (STR).[77]

Section 29[78] deals with the concepts of "knowledge" and "suspicion" and creates a reporting onus in respect of suspicious and unusual transactions. The scope of section 29 is that it applies to any person who runs, manages or works for a business. Adriaans as a director of the defendant's law firm at the time of this incident falls within this category. All the personnel of the defendant also would fall within this category, and thereby incur a legal obligation in respect of STRs. It would therefore also include those persons who did the verification in terms of FICA to determine the identity of the client Sewmach.

In particular, section 29(1)(a) places an obligation on any relevant person to file an STR pertaining to his knowledge or suspicion of the receipt or imminent receipt by the business of the proceeds of unlawful activities. Section 29(1)(b) creates identical STR obligations in respect of those business transactions which facilitate or are likely to facilitate the transfer of the proceeds of unlawful activities, or which are not manifestly lawful, or which are aimed at evading any FICA reporting duty, or which may pertain to tax evasion.[79] Section 29(1)(c) replicates the STR duty in relation to the use or imminent use of the business for money laundering purposes.[80] The STR must be filed within 15 working days of the person having become aware of the transaction in question,[81] and must contain the particulars prescribed by Regulation 23 of the FICA regulations. Section 29(2) prescribes a similar STR duty in respect of dubious transactions which, if concluded, may have caused the business to be used, *inter alia*, for money laundering purposes. In a word, then, section 29 makes the reporting to the Financial Intelligence Centre of unlawful or suspicious transactions, including money laundering transactions, mandatory for all members of a business, including a legal practice. The court should have dealt with the conduct of Adriaans in terms of section

[76] Financial Intelligence Centre Act 38 of 2001.

[77] Section 1 of FICA defines a "transaction" as "a transaction concluded between a client and an accountable institution in accordance with the type of business carried on by that institution". Although this is a quite tautologous and also otherwise problematic definition, it has the merit at least of encompassing attorneys, who head the list of accountable institutions in Schedule 1. For considerations of the difficulties entailed in the statutory definition of "transaction", see De Koker, L "Money laundering in South Africa" (2006) 90; Itsikowitz, A "Legal professional privilege/intermediary confidentiality: The challenge for anti-money laundering measures" (2006) at 78-79.

[78] See Hamman and Koen (2012) at 73.

[79] S 29(1)(b) consists of five paragraphs. Paras (i) to (iv) each may be read, in whole or in part, as money laundering controls. Para (v) deals exclusively with terrorist financing.

[80] Van der Westhuizen April 2004 *De Rebus* 37.

[81] Regulation 24 of the regulations to FICA.

29 to determine whether he should or ought to have known that the money came from a suspicious source.[82]

The failure by an attorney to file an STR in terms of section 29 is criminalised by section 51 and section 52[83] and section 68 prescribes maximum penalties for such non-reporting, namely, 15 years' imprisonment or a fine of R10 million. This is the possible penalty for attorneys convicted of the non-reporting of a suspicious and unusual transaction.

8 STEPS TO SAFEGUARD AGAINST BECOMING A VICTIM

As mentioned above money launderers are always searching for new avenues to clean their ill-gotten gains, and attorneys' trust accounts are especially appealing for such purposes.[84] Attorneys should guard against being used as pawns in this process.[85] It is in the nature of a legal practitioner's profession that some firms will have huge amounts of money in their trust accounts. Phishing can be prevented by being cautious and not opening any link contained in an e-mail, especially a link to a financial institution. Once a bank website is opened attorneys should look for the "https" sign in the web address instead of the normal "http".[86] The "s" in the "https" sign indicates that the website is secure.[87] All the major banks also have a picture of a small lock next to the internet address which indicates that the website is secure. Absa, in addition to the "s" in "https" and the lock that is displayed, also provide clients when they first log on to their bank accounts, with a "surephrase" which is displayed whenever they use the internet thereafter, to indicate that it is secure to continue with the transaction. Banks also have an "sms" notification via cellphone: whenever there is movement on an account, a client receives an sms.[88] In the unfortunate event of an attorney becoming a victim of a phishing scam, there are a number of avenues that he can pursue.

Roestof could have mitigated his damages. Two hours after he visited the bank's website he was phoned that money had been fraudulently transferred out of his account.[89] He went the next day to the bank and the police and received details of the bank account number into which the deposit had been made.[90] His banker was aware of this account number as well as the identity of the account holder. Surely, there should

[82] See discussion of section 29 reporting obligation by Hamman and Koen (2012) at 73.

[83]The criminalisation effected by s 52 includes the negligent failure to submit an STR report. It would appear that attorneys are required always to adhere to the standard of the reasonable person in relation to unusual and suspicious transactions.

[84] LAWPRO (2003) at 21. Hamman and Koen (2012) at 69.

[85] Hamman and Koen (2012) at 69.

[86] Kyrnin J "What is HTTPS" http://webdesign.about.com/od/ecommerce/a/aa070407.htm (accessed 20 March 2013) Sieber T "What Is HTTPS" http://www.makeuseof.com/tag/https-enable-secure-connections-default (accessed 20 March 2013).

[87] Phishing Scams http://www.absa.co.za/Absacoza/Security-Centre/Latest-Scams/Phishing-Scams (accessed 20 March 2013).

[88] Roestof indeed received one from Absa Bank. First National Bank calls their sms service "in contact".

[89] See *Roestof v Cliffe Dekker Hofmeyr Inc* para 28.

[90] *Roestof v Cliffe Dekker Hofmeyr Inc* para 28-30.

be mechanisms in place for banks to flag or attach a form of caveat against, such an account. In this case there is no indication that although the bank was aware of the fraudulent transaction and had contacted its client, that it assisted him in any manner in trying to minimise his loss. Banks should be encouraged to assist clients in such predicaments by furnishing them with details, such as the name of the account holder in whose account the deposit has been made. It was in fact Roestof's own bank that informed him of the fraudulent transaction, and the question arises why it did not contact the other bank in order to assist him.

The bank's negligence in this matter also did not receive much attention from the court. Banks, as accountable institutions, have the same duties as attorneys of reporting suspicious and unusual transactions. Roestof's own bank in its negligent dealing with this matter also contributed toward his loss.[91] He was phoned by his bank on the day that the money had been fraudulently transferred out of his account. The next day when he went to the bank he received details of the bank account number, but at that stage his banker, whilst being aware of the identity of the account holder, did not inform his client thereof. His bank failed to contact the defendant's bank to alert them of the fraudulent transaction. It could have sent a request to the defendant's bank to put a hold on the account as it suspected that fraud had been committed. Such a request would have given Roestof sufficient time to prepare and try to get the money back.

Attorneys, in the event of their becoming victims of phishing scams, should endeavour to approach the courts on an urgent basis to obtain a court order preventing the transfer of the money out of the account. Speed is of the essence. This phishing occurred on Thursday 14 January 2010 and the amount was only transferred out of defendant's account on Monday 18 January 2010 without anyone informing it of the situation before the transfer out of its trust account occurred.[92]

Attorneys should be more vigilant when they receive telephonic instructions, as Adriaans did in this case. The client never came to the office, and whenever money is requested to be paid out urgently, red lights should be flashing. Adriaans was fortunate that the court found no negligence on his part and that he was therefore beyond the ambit and penalties of section 29 of FICA.

9 CONCLUSION

In this case a cyber-launderer utilised an attorney's trust account to clean ill-gotten gains. It illustrates how lawyers can become an element in a money laundering scheme.[93] Attorney firms must be cautious in the operation of their trust accounts and should try to put mechanisms and safeguards in place with regard to their electronic

[91] See *Absa Bank Ltd v Lombard Insurance Company Ltd, FirstRand Bank Ltd v Lombard Insurance Company Ltd* 2012(6) SA 569 (SCA); [2012] 4 All SA 484 (SCA). Wherein the court determined that: "The legal effect of an electronic funds transfer is that no physical money changes hands, but the account holder obtains a claim against his bank for the credit on the account."

[92] *Roestof v Cliffe Dekker Hofmeyr Inc* para 36.

[93] Report on money laundering typologies 2000-2001, FATF. 14.

transactions. The *Roestof* case illustrates how easy it is to become a victim of money launderers as a result of phishing schemes and how easy it is for a launderer to use trust accounts as laundromats to clean the money.[94] Although the money which was laundered through the phishing scheme was taken out of Roestof's personal account, it may happen that attorneys who conduct transactions out of their trust accounts via the internet can become victims of launderers and their trust accounts be cleaned out. This will have huge repercussion for an attorney who will have to compensate his trust creditors and face possible criminal prosecution.

The legal profession must be aware that a money launderer is not likely to let an opportunity slip by to use an attorney's trust account as a mechanism through which to clean his money.[95] Adriaans was fortunate that the court found no negligence on his part and that he was therefore beyond the ambit and penalties of section 29 of FICA.[96] He could have been in the same position as the lawyer in *R v Griffiths,*[97] who was convicted because there were reasonable grounds for him to believe that there was something wrong with a property transaction, and that he should have reported the suspicious transaction.

If the situation arises that an attorney is found to be negligent in dealing with money that was fraudulently deposited into a trust account, such attorney will not only face a civil action from the person whose account was cleaned out via a possible phishing scam, but will also have to face possible criminal prosecution[98] and, if convicted, could face a sentence of up to 15 years' imprisonment or a fine of R10 million.[99]

BIBLIOGRAPHY

Books and chapters in books

De Koker, L *Money laundering in South Africa* in Goredema, C (ed) *Profiling Money Laundering in Eastern and Southern Africa,* Institute for Security Studies Pretoria (2003)

Itsikowitz, A *"Legal professional privilege/intermediary confidentiality: The challenge for anti-money laundering measures"* in Goredema, C (ed) *Money laundering experiences,* Institute for Security Studies Pretoria (2006)

[94] Hamman and Koen (2012) at 69.

[95] Shepherd (2002) at 26. LAWPRO (2003) at 21. *S v Hattingh* is an example of how a launderer after committing fraud, theft and money laundering arising from a property scheme, defrauded four prominent South African banks of R55 million rand.

[96] *Roestof v Cliffe Dekker Hofmeyr Inc* para 92.

[97] *R v Griffiths* [2006] All ER (D) 19.

[98] See, for example, *S v Price* 2003 2 SACR 551 (SCA); *Pillay* v S [2004] 1 All SA 61 (SCA); *S v Rossouw*, (Unreported, Wynberg Regional Court, Case Number B1679/09, SHD163/09); and *S v Hattingh*, (Unreported, Bloemfontein Regional Court, Case Number 17/518/10).

[99] S 68 of FICA.

Madinger J *Money laundering*: A guide for criminal investigators. 3ed CRC Press Boca Raton FL (2012)

Richards J *Transnational criminal organizations, cybercrime, and money laundering Boca Raton FL* CRC Press (1999)

Weatherford J *The history of money* New York, New York: Three Rivers Press (1997).

Cases

Absa Bank Ltd v Lombard Insurance Company Ltd, Firstrand Bank Ltd v Lombard Insurance Company Ltd 2012(6) SA 569 (SCA);[2012} 4 All SA 484 (SCA) 28

*Du Preez v Zwieger*s 2008 (4) SA 627 (SCA)

Hirschowitz Flionis v Bartlett and Another 2006 (3) SA 575 (SCA)

Holmes v Law Society of the Cape of Good Hope and Another 2006 (2) SA 139 (C)

Law Society, Transvaal v Matthews 1989 (4) SA 389 (T)

Law Society of the Cape of Good Hope v Peter [2006] SCA 37 .

Nissan SA Pty Ltd v Marnitz 2005 (1) SA 441 (SCA)

Pillay v S [2004] 1 All SA 61 (SCA)

Roestof v Cliffe Dekker Hofmeyr Inc (34306/2010) [2011] ZAGPPHC 219 (2012)

R v Griffiths [2006] All ER (D) 19

Summerley v Law Society, Northern Provinces 2006 (5) SA 613 SA

S v Price 2003 2 SACR 551 (SCA)

S v Rossouw, Unreported, Wynberg Regional Court, Case Number B1679/09 (SHD163/09)

S v Hattingh, Unreported, Bloemfontein Regional Court, Case Number 17/518/10

Legislation

Attorneys Act 53 of 1979

Financial Intelligence Centre Act 38 of 2001

Close Corporation Act 69 of 1984

Articles

Armstrong H L & Forde PJ (2003) "Internet anonymity practices in computer crime", *Information Management & Computer Security*, Vol. 11: 5, 209 - 215

Filipkowski W "Cyber Laundering: An Analysis of Typology and Techniques" (2008) *International Journal of Criminal Justice Sciences* Vol 3 Issue 1 January - June 2008

Fox M "Phishing, pharming and identity theft in the banking industry" (2006) 21(9), *Journal of International Banking Law and Regulation* 548

Hamman A J and R A Koen "*Cave Pecuniam:* Lawyers as Launderers" (2012) 15 (5) *PELJ* 69-100.

Hinterseer K "An Economic Analysis of Money Laundering" (1997) Vol 1:2 *Journal of Money Laundering* 154-155.

Joyce B P "e-diligence: money laundering risks in the electronic arena" (2001) 5 *Journal of Money Laundering Control* 146-149.

Ping H E "New Trends in Money Laundering -From the Real World to Cyberspace" (2004) 8 *Journal of Money Laundering Control* 48-55.

Phillippsohn S "The Dangers of New Technology- Laundering on the Internet" (2001) *5 Journal of Money Laundering Control* 87-95.

Shepherd K "USA Patriot Act Surprising implications for transactional lawyers" *Probate & Property* September 2002 26-30.

Van der Westhuizen M "Interpreting section 29 and the obligation to report" part 1 April 2004 *De Rebus* 37-38

Van Jaarsveld I L "Following the Money Across Cyber Highways: A Herculean Task or International Challenge? Some Thoughts on Money Laundering on the Internet" (2004) 16 SA *Merc LJ* 685-694

Reports

Financial Action Task Force on Money Laundering: Report on money laundering typologies 2000-2001, FATF

International Standards On Combating Money Laundering And The Financing of Terrorism & Proliferation. The FATF Recommendations, February 2012, Financial Action Task Force.

Internet Sources

Kyrnin J "What is HTTPS - Why Secure a Web Site Use HTTPS for Storefronts and Ecommerce Web Sites" http://webdesign.about.com/od/ecommerce/a/aa070407.htm

LAWPRO 2003 "Respecting the 'Trust' in Trust account" www.practicepro.ca/LAWPROMag/march2003_trusts.pdf

Phishing Scams http://www.absa.co.za/Absacoza/Security-Centre/Latest-Scams/Phishing-Scams

Sieber T "What Is HTTPS & How To Enable Secure Connections Per Default" (2011)

http://www.makeuseof.com/tag/https-enable-secure-connections-default