IN THE HIGH COURT OF SOUTH AFRICA
EASTERN CAPE DIVISION, GRAHAMSTOWN CASE NO. CA&R17/2018

In the matter between:

BONGANI MYENI **Appellant**

and

THE STATE **Respondent**

APPEAL JUDGMENT

Bloem J.

[1] The appellant and three others were charged with contravening some provisions of section 86 of the Electronic Communications and Transactions Act,[1] fraud alternatively theft and contravening section 4 of the Prevention of Organised Crime Act.[2] The state withdrew all the charges against one of the accused. The appellant and his co-accused, Lungisa Kosi and Morena Senatle, were convicted on all the counts, as charged. Each of them was sentenced to two years' imprisonment on count 1; one year imprisonment on count 2; fifteen years' imprisonment on count 3; and five years' imprisonment on count 4. The magistrate ordered the sentences on counts 1 and 2 to run concurrently with the sentence imposed on count 3. The effect thereof was that the appellant and his co-accused were each sentenced to twenty years' imprisonment.

[2] The magistrate refused applications by the appellant and his co-accused for leave to appeal against their conviction and sentence. The applications by Mr Kosi and Mr Senatle respectively for leave to appeal against their conviction and sentence were refused by this court and later the Supreme Court of Appeal. This court

[1] Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002).
[2] Prevention of Organised Crime Act, 1998 (Act No. 121 of 1998).

granted leave to the appellant to appeal against his conviction and sentence.

[3] In count 1 they were alleged to have contravened the provisions of section 86 (4) alternatively 86 (1) of the Electronic Communications and Transactions Act. Section 86 deals with unauthorised access to, interception of or interference with data. It reads as follows:

> "(1) Subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.
> (2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.
> (3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence.
> (4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.
> (5) A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence."

[4] The allegations against them in count 1 were that between December 2009 and February 2010 and in contravention of section 86 (4), they, allegedly being members of a syndicate, wrongfully and unlawfully used a device which is primarily designed to overcome security measures in place for the detection of data, namely computer software by the name of Winspy which captures keystrokes in order to overcome the security measures, designed to protect such data, namely computer usernames and passwords, without the authority of the

Koukamma Municipality (the municipality). In the alternative, it was alleged that during the above period they, in contravention of section 86 (1), unlawfully and intentionally accessed or intercepted data, namely computer usernames and passwords, without having authority or permission to do so.

[5] In count 2 it was alleged that during the above period they, in contravention of section 86 (1), unlawfully and intentionally accessed or intercepted data, namely the Random Verification Number (RVN) which was sent to an authorised employee of the municipality for onward transmission to ABSA Bank, without having authority or permission to do so.

[6] In count 3 it was alleged that during the above period they gave out and pretended to ABSA Bank that certain payments were captured, verified and released by the municipality's employees, that those payments were authorised in the normal and ordinary course of the municipality's business and that the beneficiaries of those payments were entitled to receive such payment, that, by the above misrepresentations, they induced ABSA Bank, to the actual or potential loss and prejudice of the municipality, transferred those payments to those beneficiaries, when in truth and in fact, when they so gave out and pretended, they knew that those payments were not captured, verified and released by the municipality's employees, that those payments were not authorised in the normal and ordinary course of the municipality's business, that the beneficiaries were not entitled to receive those payments and that they intended to appropriate those payments to themselves. In the alternative it was alleged that they stole the amounts paid into the beneficiaries' bank accounts from the municipality.

[7] In count 4 it was alleged that during the above period they, in contravention of

section 4 of the Prevention of Organised Crime Act, knew or ought reasonably to have known that the amounts paid into the bank accounts of the beneficiaries were or formed part of the proceeds of unlawful activities. The appellant and his co-accused pleaded not guilty to all the charges without a plea explanation.

[8] By agreement between the state, the appellant and his co-accused the magistrate received in evidence, under cover of an affidavit envisaged in section 236 of the Criminal Procedure Act,[3] bank statements and internet banking logs of the municipality for the period between 13 and 15 February 2010 as well as the bank statements of 16 beneficiaries in respect of the above payments.

[9] To prove its case, the state called various witnesses. Banele Bavu, Sisiwe Kosi and Mornay Micheals were employed by the municipality at the relevant time as an accountant, expenditure accountant and expenditure clerk respectively. They could capture and verify payments on the municipality's computer system but could not release payments. Only Sizeka Walana could release payments. Ms Walana was employed by the municipality as a senior accountant for five years until 2013 when her contract of employment expired. She testified that her main duties were to supervise the expenditure, revenue and supply chain sections of the municipality. In the expenditure section she supervised payments made by the municipality. Before a payment could be made she would check whether all documents in support of payment were available. If satisfied she authorised payment. She required a username and password to switch on her computer. To access the municipality's internet bank account and to make payment therefrom, she used a separate username and password. She changed her password on a weekly basis. It was known only by her. She and the above employees testified

[3] Criminal Procedure Act, 1977 (Act No. 51 of 1977).

that they became aware of the unauthorised payment of R1.4m from the municipality's bank account only on the day following such payment. They had no idea how and by whom those payments were made.

[10] The appellant and his co-accused then admitted, in terms of section 220 of the Criminal Procedure Act, that members of the syndicate and other persons unknown to the state conspired to commit the offences set out in the charge sheet. They targeted three of the municipality's bank accounts, by disabling the firewall of some of the municipality's computers which were used to capture, verify and release payments, by using the Winspy software to record all keystrokes including usernames and passwords. That information was then emailed to members of the syndicate who would in turn use that information to capture, verify and release unauthorised payments from the municipality's bank account into specified beneficiary accounts. They did so by also unlawfully obtaining information required by Vodacom before a SIM swop could be processed on a particular cell phone and by providing the information so obtained to Vodacom, thereby inducing Vodacom to process the SIM swop which resulted in members of the syndicate having access to the RVN which is sent by sms to the authorised employee of the municipality to release payments from the municipality's bank accounts. Vodacom would send the RVN to the authorised employee's cell phone. It is only when that employee supplies the RVN to ABSA Bank that payment would be released. The parties furthermore agreed that between 13 and 14 February 2010 members of the syndicate captured, verified and released unauthorised payment in the sum of R1.4m from the municipality's bank account into the bank accounts of sixteen different beneficiaries, that members of the syndicate approached various individuals to open new bank accounts in exchange for the promise of some

benefit and in some cases there was unlawful access to the bank accounts of various individuals and entities.

[11] The statements of eleven persons were also admitted by agreement. In those statements they described how they were approached by Thobani Khumalo and his subordinates with the promise of employment. Mr Khumalo required of them to have or open ABSA Bank accounts and to provide him with the bank cards and pin numbers of those accounts to enable the "*employer*" to pay their salaries into those accounts and to enable the employer to first withdraw its share of the income. Mr Khumalo stated that persons known to him as Charlie and Kelvin approached him to recruit "*employees for upcoming tenders*" from ABSA Bank. In his statement Mr Khumalo confirmed having recruited many persons as prospective employees. None of the recruited persons was ever employed, as promised.

[12] Simphiwe Spellman testified that during February 2010 he was employed by the municipality as its chief financial officer. At the time he was also its acting municipal manager. He was the only one who received the RVN before payments by the municipality could be released. He testified that on Saturday, 13 February 2010 he received unusually many irrelevant and unsolicited text (spam) messages on his cell phone. He received more such messages during the following morning. At approximately midday on that Sunday someone, who identified himself as a Vodacom employee, telephoned him on his cell phone. He informed Mr Spellman that his cell phone was not the only one receiving so many spam messages. The person asked him a few questions before he requested him to switch off his cell phone for two hours to attend to the problem. When Mr Spellman switched on his cell phone after two hours it reflected that his SIM card had not been inserted

although it was never removed from his cell phone. He contacted Vodacom. It turned out that while his cell phone was off a SIM swop had been effected. As a consequence telephone alerts which would have come through on his cell phone when payments were made from the municipality's bank accounts were diverted to another cell phone. Later that day Vodacom managed to reverse the SIM swop and Mr Spellman could use his cell phone.

[13] The following morning ABSA Bank called to inform him that payments totalling R1.4m had been made from the municipality's bank account during the previous day. The matter was reported to the police. The bank accounts into which payments had been made from the municipality's bank account were frozen. The entire amount of R1.4m was recovered, except for R500.00 which had in the meantime been withdrawn from an ATM.

[14] Conroy van Biljon is an investigator attached to the Cyber Crime Support Unit of the South African Police Service. He underwent many courses as part of his training coupled with many years of experience in the field of investigating cybercrimes. Warrant officer van Biljon received an Apple iPhone from the investigating officer in this case, warrant officer Meyer, with the request to extract data from it. The data was extracted and printed in various reports. He did so by using his expertise. He also testified about the reports which contained data of some of the municipality's computers. One report showed the usernames and passwords of employees who were authorised to capture and verify payments as well as those who could release payments. Another report showed the various cell phone numbers to which telephone calls had been made or cell phone numbers from which telephone calls were made to the Apple iPhone.

[15] Sipho Msomi testified that he was serving a sentence of imprisonment for having been convicted on similar charges as the ones in this matter as well as having defrauded the KwaZulu-Natal Department of Education of R4.9m and the Port Elizabeth Municipality of R19.7m. In this matter he pleaded guilty to similar charges. He was sentenced to fifteen years' imprisonment. After he was sentenced he was approached by the police to whom he gave a witness statement because, in his words, it was the right thing to do.

[16] Mr Msomi testified that he was introduced to Mr Kosi by one Duzi Mkize, a co-accused in another matter. He was arrested about a month or two after he had defrauded the Port Elizabeth Municipality. Before his arrest he and Mr Kosi were looking for people employed by a municipality or a government department to recruit to enable them to have access to its computer system to transfer funds to the bank accounts of unauthorised beneficiaries. Mr Msomi had access to his iPhone while in custody. Mr Kosi telephoned him during December 2009 to advise that he had managed to get a person who was prepared to give them access to the computer system of the municipality which employed him. With the help of an unknown administrator in the municipality's IT department, the security system of the municipality's computer network was disabled on 21 January 2010. The installation of the Winspy software, which disabled the security system, created a log file on the computer which recorded any and every activity on the computer in which it was installed. The IT administrator emailed the log files to Mr Msomi. He accessed the log files on his iPhone. Mr Msomi obtained the usernames and passwords of persons who could capture, verify and release payments from the log files. He could and did in fact use their usernames and passwords to effect electronic transfer of funds from the municipality's bank account.

[17] Mr Msomi testified that he had to deal with the RVN before the funds could be transferred from the municipality's bank account. New beneficiaries could not be added to the municipality's internet bank account without a change of the cell phone number of the person who should receive and send the RVN. Up until then the RVN was received and sent by Mr Spellman before payment was made by the municipality. Mr Msomi confirmed having sent numerous spam messages to Mr Spellman, that he later phoned him and pretended to be from Vodacom, that he told Mr Spellman that he had identified a system error affecting him and various other users, that he was working on the error and would call him back if the problem persisted. He called Mr Spellman after he had sent more spam messages to his cell phone and told him that he needed to verify some information to correct the errors. Having obtained the requested information from Mr Spellman, he requested him to switch off his cell phone for two hours. Mr Msomi sent the information that he had obtained from Mr Spellman to Mr Kosi who arranged for a SIM swop on Mr Spellman's cell phone. New beneficiaries could then be added to the municipality's bank account without Mr Spellman being alerted.

[18] Sidney Charlie testified that at the relevant time only he and Mr Senatle were employed in the IT section of the municipality. Mr Senatle was the IT manager to whom he reported. The server of the municipality's computer network was in Mr Senatle's office. Mr Charlie testified that he did not disable any firewalls of the server. That evidence was unchallenged.

[19] Willem Pretorius is also an investigator attached to the Cyber Crime Support Unit with more than twenty years' experience. He testified that the investigating officer requested him to acquire and analyse the data on the hard drives of four

computers belonging to the municipality. He testified that Winspy and eBlaster software were found on the computers of two employees, Ms Kosi being one of them. His further evidence is not relevant to this appeal. The state closed its case after the appellant, Mr Kosi and Mr Senatle had made further admissions which are also not relevant to this appeal.

[20] Only Mr Kosi testified. He denied that he was involved in the planning or execution of the offences and denied Mr Msomi's evidence to the contrary. The appellant and Mr Senatle did not testify. The magistrate convicted the appellant primarily on the evidence of Mr Msomi. She took into account that he was a single witness regarding the planning and execution of the offences and that he was an accomplice. The record reveals that she treated Mr Msomi's evidence with caution. She also took into account that he testified over several days and was subjected to lengthy cross-examination. She found that he impressed her as a very intelligent witness who "*was able to explain in a clear and comprehensive way the procedures he and the alleged accomplices followed to reach their goals*". She also took into account that while he was giving evidence, he did not deviate from the facts set out in his plea, witness statement and other admissions that he had earlier made. That, in her view, showed consistency on his part. She furthermore took into account that he did not receive any promise or special considerations in exchange for a guilty plea or witness statement, that he was friends with Mr Kosi and the appellant and that there was no trace of ill-feelings or malice towards them. The magistrate also found that his evidence was corroborated by objective facts. Since he was in prison at all material times there were aspects in the planning and executions of the offences which only a person or persons outside prison could perform. He required the assistance of a person

to physically install the software in the computers at the municipality's offices. It was Mr Senatle who installed the Winspy software, the installation of which was detected by warrant officer Pretorius. Mr Msomi also required the assistance of a person who was not in custody to do the SIM swop to bypass the RVN needed to transfer funds from the municipality's bank account. Mr Kosi was instrumental in that regard.

[21] Corroboration of Mr Msomi's version was also found in the various reports of information extracted from his iPhone, Mr Kosi's cell phone and various computers. After the magistrate had subjected Mr Msomi's evidence to close scrutiny she found it to bear the stamp of quality, truthfulness and reliability. The magistrate nevertheless pointed out that the acceptance of the evidence tendered by the state did not mean that it proved its case against the appellant and his co-accused beyond reasonable doubt. She analysed Mr Kosi's evidence and rejected it as false. Regarding the appellant and Mr Senatle, she found that Mr Msomi's evidence showed that they played active and important roles respectively in the commission of the offences and that Mr Msomi's evidence was conclusive in the absence of evidence in rebuttal thereof.[4] She accordingly found that the state proved beyond reasonable doubt that the appellant and his co-accused had acted together to achieve the common purpose of transferring money from the municipality's bank account to unauthorised beneficiaries and in the process committed the offences of which she had convicted them.

[22] Before us Ms Mazibukwana, attorney for the appellant, submitted that the magistrate should not have relied on Mr Msomi's evidence because he "*was not entirely honest*". For that submission she relied on a text message sent at 19h02

[4] *S v Boesak* 2000 (1) SACR 633 (SCA) at 646d-g.

on 25 September 2009 by one Msomi to Mr Msomi's cell phone. The message was written in Zulu. Loosely translated it read "*Brother, could you advise me what is happening, so that if it is not working I can give back the cards to their owners as they want their cards*". The criticism against Mr Msomi was firstly, that he did not testify about his dealings with the other Msomi in the commission of the offences; and secondly, that throughout his evidence, Mr Msomi denied being in possession of the bank cards of the unauthorised beneficiaries.

[23] The submission on behalf of the appellant has no factual basis and can accordingly not be sustained. Firstly, Mr Msomi was not cross-examined on that text message. It would accordingly be unfair to suggest that Mr Msomi was lying in this regard when he was not afforded an opportunity of answering questions relevant to that text message. He might have had an innocent explanation for that text message which, according to the report, was unread.[5]

[24] Secondly, that text message has nothing to do with the planning or execution of the offences in this matter. Mr Msomi's evidence was that he was introduced to Mr Kosi in Port Elizabeth during August 2009. They and others defrauded the Port Elizabeth municipality on or about 14 August 2009. Mr Msomi was arrested about two months thereafter. He testified that during the two months after the offences in respect of the Port Elizabeth Municipality had been committed, he and Mr Kosi looked for another municipality or government department to defraud. He was arrested before a municipality or department had been identified. After his arrest and while he was in custody he received a call from Mr Kosi during December 2009 who informed him that he had been able to get a person in a municipality who was willing to assist their plans. There was no evidence that there was any

[5] *S v Mavinini* 20009 (1) SACR 523 (SCA) at 527h-528a.

agreement between Mr Msomi and Mr Kosi that beneficiaries should be recruited. In any event, Mr Msomi was in custody and could not recruit beneficiaries. Logic dictates that no prospective beneficiary would have taken his or her bank card to a sentenced prisoner. The text message of 25 September 2009 could, in the circumstances, not have been related to the unauthorised transfer of funds from the Koukamma Municipality. The plan to transfer funds from the municipality took shape only from December 2009 when Mr Kosi called Mr Msomi to inform him of the person who was prepared to assist. The recruitment of beneficiaries could not have happened before then.

[25] Regarding the appellant's involvement in the commission of the offences, Mr Msomi's evidence, which the appellant elected not to rebut, was that he met the appellant in Durban during 2008 when he was introduced to him by a friend. They shared accommodation during 2009. That was when the appellant became aware of Mr Msomi's unlawful activities. Whenever Mr Msomi had to leave their shared accommodation he informed the appellant of his destination and what he intended doing there. In this case the appellant informed him that he had sent the details of his bank account to Mr Kosi, obviously to be added as a beneficiary to the municipality's bank account.

[26] The magistrate's analysis of the facts and her credibility findings in favour of Mr Msomi and against Mr Kosi cannot be faulted.[6] She correctly found, based on an assessment of all the evidence, that the state proved its case against the appellant and his co-accused beyond reasonable doubt. In the circumstances, his appeal against conviction should be refused.

[6] *S v Monyane and others* 2008 (1) SACR 543 (SCA) at 547j-548b.

[27] Ms Mazibukwana submitted that the magistrate should have placed more emphasis on the fact that the municipality did not suffer any loss, save for the sum of R500.00 which had been withdrawn from an ATM. All the funds which had unlawfully been transferred from the municipality's bank account and transferred into the bank accounts of the unauthorised beneficiaries had been frozen by ABSA Bank and returned to the municipality's bank account. Ms Mazibukwana furthermore submitted that another mitigating factor in favour of the appellant was that no money was transferred into his account. The magistrate considered both factors. That the municipality suffered loss of only R500.00 and that no funds were paid into the appellant's bank account were not because of his act or inaction. Rather, it was fortuitous. An attempt to pay R98 000.00 into his account was unsuccessful. Had it not been for the fact that the funds had been transferred from the municipality's bank account on a Sunday, the funds would have been dissipated by the appellant and others, on behalf of the unauthorised beneficiaries, as soon it had been transferred. The swift action by ABSA Bank, Mr Spellman and the police prevented the funds from being dissipated. The appellant had nothing to do with the fact that the municipality's actual loss was limited to R500.00.

[28] Ms Mazibukwana submitted that there were substantial and compelling circumstances which justified the imposition of a lesser sentence than the sentence of fifteen years' imprisonment prescribed for fraud involving an amount of more than R500 000.00.[7] That the appellant did not benefit from the offences, that he played a lesser role than, for instance, Mr Senatle, that he was the father of three minor children, that he was earning a salary of R8 000.00 per month, that he had no previous convictions do not, in my view, constitute substantial and

[7] Section 51 (2) (a) (i) of the Criminal Law Amendment Act, 1997 (Act No. 105 of 1997).

compelling circumstances justifying a lesser sentence than the sentence prescribed. The appellant was convicted of serious offences. Ms Mazibukwana did not make submissions to the contrary. The magistrate took the appellant's personal circumstances into account. Members of society expect courts to treat person who steal from the public purse harshly. Such money is intended for much needed services to be delivered by municipalities. In this matter the appellant and others planned the commission of these offences over a long period. Taking into account the appellant's personal circumstances, that he had been convicted of serious offences and society's interests, I am of the view that the sentences imposed by the magistrate were appropriate. There is no reason to interfere with the sentences imposed by her.

[29] In the result, the appeal against convictions and sentences is dismissed.

_____

G H BLOEM
Judge of the High Court

JAJI, J

I agree.

_____

N P JAJI
Judge of the High Court

For the appellant:	Ms N M Mazibukwana of Legal Aid South Africa, Grahamstown.
For the respondent:	Adv U de Klerk of the office of the Director of Public Prosecutions, Grahamstown.
Date of hearing:	24 October 2018.
Date of delivery of the judgment:	1 November 2018.