IN THE HIGH COURT OF SOUTH AFRICA

EASTERN CAPE DIVISION, GRAHAMSTOWN CASE NO. CA & R 117/16

In the matter between:

BENSON OKUNDU **Appellant**

and

THE STATE **Respondent**

JUDGMENT

Bloem J.

[1] The appellant was charged with and convicted in the regional court on five counts (1 to 5) of fraud, two counts (6 and 7) of the contravention of section 86(1) of the Electronics Communications and Transactions Act[1] (the ECTA), five counts (8 to 12) of the contravention of section 86 (4) of the ECTA, two counts (13 and 14) of the contravention of section 45 of the Regulation of Interception of Communications and Provision of Communication-related Information Act[2] (RICA) alternatively contravention of section 86 (3) of the ECTA and one count (15) of the contravention of section 36 of the General Law Amendment Act[3].

[2] The following counts were taken together for purposes of sentence in respect whereof the appellant was sentenced as follows:

2.1. counts 1, 2 and 3, three years' imprisonment;

2.2. counts 4 and 5, three years' imprisonment;

[1] Electronics Communications and Transactions Act, 2002 (Act No. 25 of 2002).
[2] Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002).
[3] General Law Amendment Act, 1955 (Act No. 62 of 1955).

2.3. counts 6 and 7, twelve months' imprisonment;

2.4. counts 8, 9, 10, 11 and 12, five years' imprisonment;

2.5. counts 13 and 14, five years' imprisonment; and

2.6. count 15, twelve months' imprisonment.

[3] The sentences on counts 1 to 5 and 15 were ordered to run concurrently and the sentences on counts 6 to 14 were ordered to run concurrently. The result was that the appellant was sentenced to an effective term of eight years' imprisonment. With the leave of the trial court the appellant appeals against his conviction on counts 8 to 15 and the sentences imposed in respect of counts 6 to 15.

[4] Although the appellant does not appeal against his conviction on counts 1 to 7, it is necessary, for purposes of the submissions made, to briefly set out the facts relevant thereto. Insofar as counts 1, 2 and 3 are concerned, the evidence adduced by the state demonstrated that at 08h55, 09h02 and 09h04 on 13 January 2014 and at Pick 'n Pay, Gonubie the appellant unlawfully, falsely and with the intent to defraud American Express, United States of America (the bank) represented to the bank that the debit card which he used to make purchases of R201.93, R248.00 and R180.00 was an original card. He furthermore misrepresented that he was the lawful cardholder and that he was entitled to make the above purchases, inducing the bank, by the above misrepresentation, to its prejudice and/or the prejudice of the real cardholder, to accept the misrepresentation as true and correct and to process the transactions, when he knew in truth and fact that the card which he used was not the original one but

that it had been forged, that he was not the lawful cardholder and that he was not authorised to make the purchases.

[5] Insofar as counts 4 and 5 are concerned, the evidence demonstrated that at 08h35 and 10h14 on 24 March 2014 and at Vodashop at East London airport the appellant unlawfully, falsely and with the intent to defraud China Construction Bank, China and St George's Bank and Company Incorporated, Panama City respectively (the banks) represented to them that the cards in his possession which he used to make purchases of R12 000.00 and R19 093.00 were original cards issued by the banks. He furthermore represented that he was the lawful cardholder and that he was entitled to make the purchases, inducing the banks, by the above misrepresentation, to their prejudice and/or the prejudice of the real cardholders, to accept the misrepresentation as true and correct and to process the transactions, when he knew in truth and fact that the cards which he used were not the original ones but that they had been forged, that he was not the lawful cardholder and that he was not authorised to make the purchases.

[6] The appellant was convicted on counts 6 and 7 because he contravened the provisions of section 86 (1) of the ECTA[4] in that on 13 January 2014 and 24 March 2014 he unlawfully gained access to data, namely information of the clients to whom the above banks issued the original cards, such information having been encoded on the magnetic strips of the original cards. The appellant had neither the authority nor the consent of the lawful cardholders and/or the banks to do so.

[4] Section 86 (1) of the ECTA provides that a person who intentionally accesses or intercepts any data without any authority or permission to do so, is guilty of an offence.

[7] The facts underlying counts 6 and 7 are that the appellant presented a Visa debit card issued by Nedbank to Pick ‘n Pay and Vodashop on 13 January 2014 and 24 March 2014 respectively. The evidence was that when he presented the debit card to Pick ‘n Pay the correct data contained on the magnetic strip of the debit card had already been deleted or altered. The data belonging to an American Express card issued by American Express, United States of America was unlawfully encoded on the magnetic strip of the Visa debit card issued by Nedbank. In other words, the Visa debit card which the appellant presented to Pick ‘n Pay was cloned with a card issued by American Express. Data encoded on the magnetic strip of the card issued by American Express was unlawfully transferred to the Visa debit card. It was testified that usually a handheld scheming device is used to transfer the data from one card to another. When the appellant presented the Visa debit card to Pick ‘n Pay and Vodashop respectively, he intentionally accessed the lawful cardholders’ data held by the relevant bank, such access having been without authority or permission. He was accordingly guilty of the offence created by section 86 (1) of the ECTA.

[8] On counts 8 to 12 the appellant was convicted of having committed offences in contravention of section 86 (4) of the ECTA which, for purposes of this appeal, reads as follows:

> “*A person who utilises any device … in order to unlawfully overcome security measures designed to protect such data …, is guilty of an offence*.”

[9] On the assumption that the Visa debit card which was presented to Pick ‘n Pay and Vodashop respectively was a device, there can be no doubt that, on the evidence, when the appellant presented it, it was utilised in order to unlawfully

overcome the security measures that the banks took to protect the lawful cardholder's data. In my view, despite those contraventions, the appellant should not have been convicted on counts 8 to 12 because such convictions constituted a duplication of the convictions on counts 1 to 5.

[10] The starting point to assess whether or not there has been an improper splitting of charges would be the definition and/or elements of the offence of fraud and the offence created by section 86 (4) of the ECTA. Fraud consists in unlawfully making, with intent to defraud, a misrepresentation which causes actual prejudice or which is potentially prejudicial to another.[5] The essential elements of fraud are: unlawfulness; making a misrepresentation; causing; prejudice or potential prejudice and intent to defraud.[6] The appellant was convicted on counts 1 to 5 because he unlawfully made misrepresentations to the banks with the intent to defraud them, which misrepresentations caused prejudice to them and/or the lawful cardholders. In other words, the appellant made the misrepresentations when he was aware of the falsity of such misrepresentations, the intention having been to deceive the banks and get them to act on the induced misrepresentations.[7] The *actus reus* of the offence consists of the use of the Visa debit card. The appellant used that specific card because he knew that it had been tampered with such that it would overcome the security measures designed by the banks to protect the lawful cardholders' data.

[11] In terms of section 86 (4) of the ECTA a person commits an offence when he utilises any device which is designed primarily to overcome security measures for

[5] JRL Milton *South African Criminal Law and Procedure* Third Edition Vol II at 702, which definition was referred to in *S v Gardener* 2011 (4) SA 79 (SCA) at 86G.
[6] JRL Milton *South African Criminal Law and Procedure* (*supra*) at 707.
[7] *Ex Parte Lebowa Development Corporation Ltd* 1989 (3) SA 71 (T) at 101D-E.

the protection of data, in order to unlawfully overcome security measures designed to protect such data or access thereto. In my view, to establish the commission of an offence in terms of section 86 (4) the state must prove that:

11.1. the accused utilised a device;

11.2. the device was designed primarily to overcome security measures;

11.3. the security measures are in place to protect data; and

11.4. the device was utilised to unlawfully overcome the security measures.

[12] Frederick Herbst, employed in the card division of Standard Group Forensics, testified on behalf of the state. For the last fourteen years he undertakes investigations relevant to credit and debit cards, card fraud and clone cards. His evidence was that when a card is issued by a bank to the lawful cardholder, the magnetic strip contains security measures to protect the lawful cardholder's data. That was the position with the Visa debit card with which purchases were made in this case. The data that was originally encoded on the Visa debit card had been unlawfully deleted and altered, he testified. Data belonging to the cards of lawful cardholders was unlawfully intercepted and encoded on the magnetic strip of the Visa debit card. It was cloned with the cards of lawful cardholders. When the Visa debit card was cloned, the cloning enabled the Visa debit card to overcome the security measures that the banks designed to protect the data of the lawful cardholders.

[13] When the appellant used the Visa credit card at Pick 'n Pay and Vodashop he unlawfully and with the intention of defrauding the banks, made a

misrepresentation to the banks that he was the lawful cardholder. Such misrepresentation caused prejudice to the banks and/or the lawful cardholders. All the elements of fraud having been satisfied, the appellant was correctly convicted of fraud. The appellant must have known that the banks take security measures to protect their clients' data. The only way for him to make the purchases at Pick 'n Pay and Vodashop was for him to use the Visa credit card in order to unlawfully overcome the security measures designed by the banks to protect the lawful cardholders' data. He accordingly committed the offence envisaged in section 86 (4) of the ECTA.

[14] It is apparent from the above exposition of the two offences that the magistrate used the same evidence necessary to convict the appellant of fraud to also convict him of the contravention of section 86 (4) of the ECTA. Furthermore, in both cases the appellant's intention was to defraud the banks and/or the lawful cardholders. In my view there has been an improper splitting of charges. Against the background of the facts found proved by the magistrate, the appellant could be convicted either of fraud or the contravention of section 86 (4) of the ECTA, not both. Since he was convicted of fraud (against which he did not appeal), his conviction on counts 8 to 12 must be set aside.

[15] In counts 13 and 14 the appellant was convicted of having possessed a listed equipment in contravention of section 45 of the RICA, which reads as follows:

> "***45 Prohibition on manufacture, possession and advertising of listed equipment***
>
> *(1) Subject to subsection (2) and section 46, no person may manufacture, assemble, possess, sell, purchase or advertise any listed equipment.*
>
> *(2) Subsection (1) does not apply to any telecommunication service provider or other person who, or law enforcement agency which, manufactures, assembles, possesses, sells, purchases or advertises*

> *listed equipment under the authority of a certificate of exemption issued to him or her or it for that purpose by the Minister under section 46*."

[16] Section 45 (2) does not apply to the facts of this case because the appellant is neither a telecommunication service provider, nor was he proven to have possessed the bank card under authority of a certificate issued to him under section 46. Section 46 (1) reads as follows:

> "***46 Exemptions***
> *(1) (a) The Minister may, upon application and in consultation with the relevant Ministers, exempt any-*
> *(i) internet service provider from complying with section 30 (4) in respect of the facilities and devices referred to in section 30 (2) (a) (ii);*
> *(ii) telecommunication service provider or any other person from one or all of the prohibited acts referred to in section 45 (1); or*
> *(iii) law enforcement agency from the prohibited acts of possessing and purchasing referred to in section 45 (1),*
> *for such period and on such conditions as the Minister determines*."

[17] There is also no evidence that the Minister of Justice and Correctional Services made the exemptions contemplated in section 46. For purposes of this application section 45 (1) means that no person may possess any listed equipment.

[18] In terms of section 1 of the RICA 'listed equipment' means any equipment declared to be listed equipment under section 44 (1) (a), and includes any component of such equipment. Section 44 (1) (a) reads as follows:

> *"**44 Listed equipment***
> *(1)(a) The Minister must, by notice in the Gazette, declare any electronic, electro-magnetic, acoustic, mechanical or other instrument, device or equipment, the design of which renders it primarily useful for purposes of the interception of communications, under the conditions or circumstances specified in the notice, to be listed equipment*."

[19] On 29 December 2005 the then Minister of Justice and Constitutional Development, acting in terms of section 44 (1) (a) declared, by notice in the

Government Gazette, certain items to be listed equipment. According to item (1) of column 2 of the Schedule of the declaration, listed equipment would be:

> "*Any instrument, device or equipment which is capable of being used to access, record, monitor or retrieve communications from a computer, without the permission of the author of the communication, including but not limited to –*
>
> *(a) keystroke recorders: and*
> *(b) software that can be installed on a computer and which has the ability to retrieve and/or store information so as to make it available to another person without the consent of the author of the communication*." (own underlining)

[20] The question is whether the Visa debit card that the appellant presented to Pick 'n Pay and Vodashop is an in instrument, device or equipment. In my view, it certainly is any one of the three. I prefer to refer to it as a device. The more important question is whether that device is capable of being used to access communications from a computer, without the permission of the author of the communications. "Communication" includes both a direct communication and an indirect communication. An "indirect communication" means the transfer of information, including a message or any part of a message, whether in the form of data that is transmitted in whole or in part by means of a postal service or a telecommunication system.[8]

[21] The state did not lead evidence to show that the Visa debit card was capable of being used to access communications from a computer. To secure a conviction under section 45 (1) of RICA the state was required to show, through evidence, that, when the appellant handed the Visa debit card to Pick 'n Pay and Vodashop, there was communication between Pick 'n Pay and Vodashop and the banks' computers. The state was required to show that that communication was

[8] See the definitions of "communication", "direct communication" and "indirect communication" in section 1 of the RICA.

in the form of Pick ‘n Pay informing the bank’s computer that the lawful cardholder wanted to purchase goods to the value of R201.93, R248.00 and R180.00 and the bank’s computer responding that there was sufficient funds in the lawful cardholder’s banking account, hence the approval of the transactions. Had that evidence been led by the state the finding might have been made that the Visa debit card is a listed equipment because it would then have been shown that it was capable of being used to access communication from a computer. Since the state failed to prove that the debit card had the above capability, it failed to prove that the card was a listed equipment with the result that it failed to prove the offence created by section 45 (1) as read with section 51 (1) (a) (i) of the RICA.

[22] The appellant was charged, in the alternative to section 45 of RICA, with the contravention of section 86 (3) of the ECTA, which, for purposes of this appeal, reads as follows:

> “*(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.*”

[23] For purposes of this appeal, a person is guilty of an offence in terms of section 86 (3) if he unlawfully possesses any device which is designed primarily to overcome security measures for the protection of data. On the basis of what is set out above when I dealt with the duplication of charges, I am of the view that in this regard the state proved its case against the appellant beyond reasonable doubt. He was in possession of the Visa debit card even before he made the

purchases (in other words, even before he committed fraud with that card or even before he accessed the lawful cardholders' data). That Visa debit was designed to overcome the security measures that the banks took to protect lawful cardholders' data. In the circumstances, the appellant should not have been convicted of the contravention of section 45 of the RICA, as stated above. He should have been convicted of the contravention of section 86 (3) of the ECTA.

[24] Since the appellant should have been convicted of the unlawful possession of the Visa debit card in contravention of section 86 (3) of the ECTA, it would amount to an improper splitting of charges were the conviction of the contravention of section 36 of the General Law Amendment Act to be upheld. That section reads as follows:

> "**36 Failure to give a satisfactory account of possession of goods**
>
> Any person who is found in possession of any goods, other than stock or produce as defined in section *one* of the Stock Theft Act, 1959 (Act No. 57 of 1959), in regard to which there is reasonable suspicion that they have been stolen and is unable to give a satisfactory account of such possession, shall be guilty of an offence and liable on conviction to the penalties which may be imposed on a conviction of theft."

[25] For an accused person to be convicted of the offence envisaged in section 36, the state must prove that he was found in possession of the item (goods), the person who found the accused had a reasonable suspicion that the goods had been stolen and the accused was unable to give a satisfactory account of his possession of the item.[9]

[26] Insofar as the accused is concerned, all that the state is required to prove is that he was found in possession of the item and that he was unable to give a satisfactory account of his possession thereof. It has already been found that the

[9] *Rex v May* 1924 OPD 274, referred to with approval in *R v Ismail and another* 1958 (1) SA 206 (A). See also *S v Naidoo* 1970 (1) SA 358 (A).

appellant was in unlawful possession of the Visa debit card. The evidence of Warrant Officer Schonknecht was that, when he arrested the appellant in respect of his unlawful possession of the Visa debit card, the appellant said that it was his card. He did not believe the appellant and arrested him. The state proved that the appellant was not the lawful holder of the Visa debit card. The only issue remaining is whether the appellant's inability to give a satisfactory explanation for his unlawful possession of the Visa debit card should cause him to be convicted of the offence envisaged in section 36, despite the fact that he has already been convicted of the unlawful possession of that card in terms of section 86 (3) of the ECTA. In my view, it will also amount to an improper splitting of charges if the appellant's conviction on count 15 were to be upheld in the face of his conviction under section 86 (3) of the ECTA. His conviction on count 15 should accordingly be set aside.

[27] Regarding the sentence which must be imposed on the contravention of section 86 (3) of the ECTA, section 89 (1) of the ECTA provides that a person convicted of an offence referred to in section 86 (3) is liable to a fine or imprisonment for a period not exceeding twelve months. In my view, regard being had to the seriousness of the offence, a term of imprisonment of twelve months on each count would be appropriate. However, the sentences on those two counts should run concurrently.

[28] In the circumstances, the following order is made:

28.1. The appeal against the conviction and sentence on counts 8 to 12 is upheld with the result that the convictions and sentences on those counts are set aside.

28.2. The appeal against the conviction and sentence on counts 13 and 14 is upheld with the result that the conviction and sentence on those counts are set aside and replaced with the following:

> "In respect of counts 13 and 14 the accused is convicted of contravening section 86 (3) of the Electronics Communications and Transactions Act.
>
> The accused is sentenced to a term of imprisonment of twelve months on each of count 13 and 14, the sentences on those two counts to run concurrently."

28.3. The appeal against the conviction and sentence on count 15 is upheld with the result that the conviction and sentence on that count is set aside.

28.4. The appellant is accordingly sentenced to an effective term of imprisonment of four years antedated to 23 September 2015.

_____

G H BLOEM
Judge of the High Court

Mbenenge J,

I agree

_____

S M MBENENGE
Judge of the High Court

For the appellant:	Adv S D Slabbert, instructed by J H Slabbert Attorneys, Durban North.
For the state:	Adv W Jaftha of the Specialized Commercial Crime Unit, East London
Date of hearing:	9 November 2016
Date of delivery of the judgment:	22 November 2016