Baker McKenzie.

Submission

Date: 5 October 2023

To: The Portfolio Committee on Justice and Correctional Services
Ricabill@parliament.gov.za

From: Baker & McKenzie Inc. on behalf of Premium Ideas South Africa (Pty) Ltd

Re: **Submission on the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill [B28—2023]**

A. Introduction

1. We refer to the Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill, which was published by the Minister of Justice and Correctional Services on 25 August 2023 (the **Bill**).[1]

2. This submission is made on behalf of Premium Ideas South Africa (Pty) Ltd (**PISA**) to the Portfolio Committee on Justice and Correctional Service (**Committee**) in relation to the Bill. PISA is South Africa's largest specialised telecommunications SIM-card fulfilment house, performing *inter alia*, SIM-card packaging and logistics services. A large part of PISA's business comprises the packaging of pre-paid SIM-cards for large mobile network operators (**MNOs**),[2] classified as "*electronic communications service providers*" under the Regulation of Interception of Communications and Provision of Communication-Related Information Act (**RICA**).

3. As a result, the manner in which RICA applies to MNOs, particularly insofar as RICA regulates the provision and activation of SIM-cards to end-users in the mobile telecommunications market, is also adhered to by PISA, as dictated by MNOs through their commercial terms. It follows that the Bill is of particular significance to PISA.

4. PISA appreciates the need for amendments to RICA in response to the Constitutional Court's ruling in *AmaBhungane Centre for Investigative Journalism and Others v Minister of Justice and Correctional Services and Others* (***AmaBhungane***).[3] While PISA is cognisant that the Bill is responsive, in particular, to the issues raised in *AmaBhungane*, we are of the view that there is a need for further amendments to RICA, which amendments have not yet been captured in the Bill.

5. We believe the Bill presents an opportunity to also address certain shortcomings or loopholes in RICA. These issues, which are of utmost public importance, relate in particular to the regulation of MNOs and their obligations through the provision of SIM-cards and SIM-card related information as provided for in section 40 of RICA. Through this submission, we hope to facilitate the broadening of the Bill's scope, and in so doing to make provision for amendments that specifically address the gaps in section 40 of RICA.

6. That said, we also make our submission on the basis that the Bill seeks to provide "*procedures to be followed for processing, examining, copying, sharing, disclosing, sorting through, using, storing or destroying of any data*". In the alternative, our submission ought to be considered by the Committee, given the necessary amendments required to regulate the provision of SIM-card information in the market, which amendments are underpinned by the judgment in *AmaBhungane*.

---

[1] Bill 28 of 2023, published in Government Gazette No. 49189 of 25 August 2023.
[2] For example, Mobile Telephone Networks (**MTN**), Vodacom, Cell C, and Telkom.
[3] 2021 (3) SA 246 (CC).

B. Summary of concerns with RICA

7. RICA provides for the regulation of interception of communications. As the Constitutional Court aptly put in *AmaBhungane*, "[RICA's] *purpose is to investigate and combat serious crime, guarantee national security, maintain public order and thereby ensure the safety of the Republic and its people*." It is plain that the purpose of RICA is to fulfil a crucial function in investigating and preventing serious crime and in ensuring the safety of the nation.

8. Despite these noble goals, RICA, as the relevant legislative framework, falls short in meeting these goals. In particular, it does not allow the South African government and its stakeholders to:

   8.1. adequately and properly carry out their law enforcement duties, in that:

      8.1.1. MNOs are unable to assist law enforcement authorities in intercepting communications;

      8.1.2. there is a perception (fact, speculation or otherwise), widely alleged in the mainstream media,[4] that MNOs facilitate the distribution of *pre-RICA'd* SIM-cards through their distributor networks or, at the very least, facilitate an environment that enables MNOs to bypass those obligations which are in fact imposed on electronic communications service providers by RICA;

   8.2. prevent the illegal transfer of funds; and

   8.3. adequately monitor and contain anti-money laundering (**AML**) risks and comply with global AML/counter-terrorism financer (**CTF**) policies.

9. PISA believes that these issues are easily remedied through simple packaging and security requirements, which we have detailed further below.

C. RICA and the regulation of SIM-cards and SIM-card related information

10. RICA directly applies to and regulates MNOs insofar as they are *electronic communication service providers*, by requiring MNOs to process, record, store and verify certain information of their customers before activating any SIM-card.[5] The particular obligations are set out in section 40 of RICA, which we have detailed more fully below.

   10.1. In order to activate a SIM-card, an MNO **must record and store the following information**:[6]

      10.1.1. the Mobile Subscriber Integrated Service Digital Network number (**MSISDN - number**) of the SIM-card that is to be activated;

---

[4] We have incorporated several mainstream media reports into this submission by way of hyperlinks contained throughout this document. To the extent that the hyperlinks may become unavailable or inaccessible to the Committee, we have also included these media reports in **Appendix A** to this submission.

[5] A SIM-card, for the purposes of RICA, is: "…*the Subscriber Identity Module which is an independent, electronically activated device designed for use in conjunction with a cellular phone to enable the user of the cellular phone to transmit and receive indirect communications by providing access to telecommunication systems and enabling such telecommunication systems to identify the particular Subscriber Identity Module and its installed information.*"

[6] Section 40(2) of RICA.

Baker McKenzie.

10.1.2. the full names and surname, identity number or passport number and at least one address of such person who requests a SIM-card; and

10.1.3. in the case of a juristic person, the full names, surname, identity number and an address of the authorised representative of the juristic person and the name and address of the juristic person and, where applicable, the registration number of the juristic person.

10.2. An MNO must **verify** the above information with reference to:[7]

10.2.1. an identification document, a registration document, founding statement, document issued by the South African Revenue Service or any other similar document;

10.2.2. a bank statement, a municipal rates and taxes invoice, telephone or cellular phone account of not older than three months, or any other utility bill or an account of a retailer of not older than three months, or an existing lease, rental or credit sale agreement, insurance policy, a current television licence or a new motor vehicle licence document; and

10.2.3. the authority of the representative of the juristic person by means of a letter of authority or an affidavit.

10.3. MNOs are required to ensure that the aforementioned information, the process by which it is obtained, and the facility in or on which it is stored, **is secure and accessible only to persons specifically designated by the MNO** in question.[8] The Minister, in consultation with the Cabinet Member responsible for communications, by notice in the Gazette, may determine security standards relating to the matters contemplated in 40(4)(a).[9]

10.4. Where any customer (i.e. a registered user of an activated SIM-card) sells or in any manner provides an *activated* SIM-card to a person (*other* than a family member), that customer must provide the electronic communications service provider with the full names, surnames, identity number and the information in section 40(2).[10]

10.5. The MNO must then **verify**, in terms of section 40(6):

10.5.1. basic identification information with reference to identity documents;

10.5.2. address information with reference to bank statements, municipal rates, cell phone account, utility bill or an account of a retailer; and

10.5.3. the MSISDN-number of the SIM card.

10.6. Once verified, the MNO must **store** this information for a period of five years[11] including every MSISDN-number used with every IMEI-number and every IMEI-number used with every MSISDN-number.[12]

[7] Section 40(3) of RICA.
[8] Section 40(4)(a).
[9] Section 40(4)(b).
[10] Section 40(5).
[11] Section 40(6) read with section 40(10).
[12] Section 40(9).

Baker McKenzie.

11. The sum and substance of the above is that in terms of section 40, **no SIM-card should be activated to a particular user unless the relevant identification information of that user is known to and verified by the MNO**.

D. Current market practices

(i) Packaging and distribution

12. In large part, all MNOs provide SIM-cards to pre-paid and post-paid subscribers. Insofar as the pre-paid SIM-card market is concerned, MNOs have historically, either themselves or through third parties, managed the distribution of pre-paid SIM cards into the market by ensuring that each pre-paid SIM-card is securely packaged.[13]

13. Pre-paid SIM-cards are packaged by market players such as PISA at secure facilities, where *unpackaged* SIM-cards are received from the MNOs' manufacturers and those SIM-cards are then packaged into tamper-proof plastic blister packs subject to the insertion of MNOs' prescribed collateral into each pack. Packagers then distribute pre-paid SIM-cards to MNOs' distribution channel partners, who pass those SIM-cards on either to their own sub-distributors, who in turn facilitate the entry of packaged pre-paid SIM-cards into the formal and informal retail markets, or directly to retailers in the formal and informal markets (from which point they are sold to consumers).

14. The packaging of SIM-cards serves a range of purposes in ensuring the secure distribution of SIM-cards to pre-paid customers, including by:

    14.1. protecting unique identifying and security information attaching to each SIM-card;

    14.2. ensuring, through the use of what is known as "*collateral*", that MNOs' terms and conditions and the requirements of RICA are communicated to pre-paid customers in conjunction with each SIM-card; and

    14.3. giving assurance to the end-user that the SIM-card is safe to use (not having the ability to be comprised).

(ii) Pre-registration

15. Distinct from packaging and distribution, the sale of SIM-cards into the pre-paid market is driven by incentives linked to the *pre-registration* of SIM-cards (i.e. pre-RICA'd SIM cards). This is a function of the current incentive and rebate model. Immediate rebates on wholesale SIM-card prices are fed to distributers and retailers upon activation of SIM-cards, following which each player in the distribution and retail chain receives a percentage of the revenue generated from the use of airtime and mobile data on a given SIM-card.

16. RICA naturally constitutes a barrier to these activation quotas and targets. Proper registration must take place before the activation of a SIM-card. It is widely accepted that many users do not possess the requisite documentation to carry out the RICA registration (either immediately at the point of sale or at all) and the logistical difficulties attendant in having to either register in-store or online before being able to make use of a SIM-card adds on to the administrative burden.

[13] The distinction between pre-paid and post-paid is made primarily because in the case of post-paid SIM-cards, the subscriber enters into a contract with the MNO in-store, and the RICA registration process is undertaken as a pre-requisite for subscription, usually by the MNO itself.

17. The result of the above is that distributors and retailers are incentivised to pre-RICA SIM-cards prior to their sale to the end-user:

17.1. This is typically carried out by third parties who use generic details to register large numbers of SIM-cards. Pre-activation of SIM-cards is exactly at odds with the import of section 40 of RICA and with RICA as a whole. It is however a routine practice, particularly in the informal distribution and retail channels, with pre-activated SIM-cards colloquially being referred to as "*pre-RICA'd*" SIM-cards. In terms of numbers:

17.1.1. it has been reported that a large distributor can receive as many three million sim cards from an MNO per month; and

17.1.2. more recently, the Business Day reported that the vast majority of the 165 million or so SIM cards that enter the market annually may be non-compliant with RICA.[14]

17.2. The practice of distributing pre-RICA'd SIM cards causes the demand at distribution and retail level to skew almost exclusively towards *unpackaged* SIM-cards, because packaging renders the pre-RICA process more cumbersome, and also limits the number of SIM-cards that can be distributed at a time from a logistical level. MNOs have tended to heed this shift in demand, with the result that the majority of SIM-cards that are released into the pre-paid market are released to distributors and retailers without any protective or other packaging.

(iii) The loophole in RICA

18. While pre-RICA'd SIM-cards are contrary to RICA, they continue to proliferate in the market because of an ostensible loophole in section 40 of RICA:

18.1. Section 40(5) enables a "*customer*" (i.e. a registered end-user of an activated SIM-card) to sell or otherwise provide a registered SIM-card to another user, subject to an obligation conferred on the customer and the new user to provide their respective relevant information to the applicable MNO for verification.

18.2. Although non-compliance with section 40 of RICA is a criminal offence, the shift in the onus to the customer and to the new user invariably means that the onus will never be discharged by either party, and the details of the new user of the SIM-card will never be provided to, stored, or verified by the issuer of the SIM-card.

18.3. In the context of pre-RICA'd SIM cards at retail and distribution levels in the pre-paid market, the "*customer*" is either the retailer or the distributor, who registers large volumes of SIM-cards under generic information. It is widely accepted that these pre-RICA'd SIM-cards are typically registered in the name of a single close corporation or company, which in some cases may serve as a special purpose vehicle specifically for the purpose of RICA registrations, and in other cases registration may be in the name of a natural person, sole proprietor, or other juristic person.

19. The mechanism of section 40(5) is accordingly an attractive proposition for MNOs, distributors, and retailers, lending itself to exploitation, in that:

19.1. the sheer number of private persons, informal retailers, and distributors who are captured by section 40(5), renders any attempts at policing compliance with section 40(5) untenable;

[14] This is notwithstanding that statistically speaking, this means that there is almost three SIM-cards allocated per person, annually.

19.2. an MNO cannot be held liable because of the shift in onus to the previous customer and new end-user;

19.3. it enables mass activation of SIM-cards without the need for consumer-specific information;

19.4. it creates a demand for unpackaged and unsecured SIM-cards; and

19.5. there is of course no regulation arising from RICA addressing the manner in which SIM-cards are to be registered as between two different users and the packaging of SIM cards to prevent the disclosure of personal information, which information can be exploited in fraudulent activities.

(iv) The effect of the loophole

20. At its core, the loophole (or Achilles' heel) in RICA leads to the proliferation of unpackaged, duplicated and/or pre-RICA'd SIM-cards. The consequences of this are manifold.

20.1. **First**, MNOs are unable to assist law enforcement authorities in intercepting communications.

20.1.1. While all of the required information and documentation for the initial end-user in section 40 is made available and stored by the MNO, the information itself is no longer useful for the purpose for which it is intended; the pre-RICA'*ing* of SIM cards means that the MNO is simply provided with the same end-user information across a vast number of SIM-cards.

20.1.2. Since an immense number of SIM-cards are sold on this basis and not transferred into the names of the end-users, the majority of SIM-cards in circulation in the pre-paid market are in reality untraceable to their end-users.

20.1.3. This effectively defeats the objectives and purposes of RICA. While RICA envisages that MNOs will be able to assist law enforcement in tracing and intercepting criminal activity, the exploitation of the loophole in RICA means that:

20.1.3.1. MNOs are unable assist law enforcement authorities in the manner intended or at all; and

20.1.3.2. the South African government and its stakeholders are prevented from adequately and properly carrying out their law enforcement duties.

20.1.4. Where transactions or communications conducted (by using a SIM-card) cannot be traced to individuals, criminals and terrorist organisations are able to abuse the anonymity associated with pre-activated SIM-cards, in consequence of which the commission and financing of crimes becomes easier, while combatting crimes becomes more difficult.[15]

[15] See media reports here and here.

20.1.5. The increase in the release of unpackaged and pre-RICA'd SIM cards into the market has also meant a concomitant increase in the practice of SIM-card cloning,[16] being the process by which a SIM-card is physically intercepted and cloned by one person before it is sold or otherwise provided to the ultimate user, which user's information is then compromised and exposed to use in criminal activity by the duplicating party. This no doubt makes easier the commission of cyber-crimes, non-criminal malicious cyber-related activities, harassment or stalking practices, social media malpractices and other undesirable online conduct.

20.1.6. Stated differently, RICA, at least in its current formulation, does not assist law enforcement officials in identifying agents and perpetrators in combatting crimes.

20.2. **Second**, government and law enforcement officials are hamstrung in their duties to prevent the illegal transfer of funds.

20.2.1. SIM-cards, beyond their basic capabilities, contain functionality that permits users, including unbanked users, to store and remit money both locally and across borders through the use of mobile phones. Given the electronic communication and money remittance capabilities of SIM-cards, SIM-cards are typically more useful for money transfers than bank cards or accounts (this in itself is indicative of the need for more stringent regulation of the dissemination of SIM-cards). As such, SIM-cards are increasingly being used within the banking and payments systems as identifiers for payments. By way of example, PayShap's ShapID can be linked to a user's mobile telephone number, enabling one person to transfer funds to another by using only the recipient's mobile number.

20.2.2. The dissemination of unpackaged SIM-cards in large volumes, without concealing or obscuring critical and sensitive information (such as MSISDN- and ICCID-numbers), creates a substantial (and foreseeable) risk that the information associated with these SIM cards, as well legitimate end users' personal information, will be compromised, as is the interception and tracing of communication emanating from these SIM-cards. This is in circumstances where the foreseeable risks (of releasing MSISDN- and ICCID-numbers indiscriminately into the market) can be easily mitigated by adopting basic and inexpensive measures, such as secure packaging, to safeguard against their compromise.

20.2.3. Cloned SIM-cards, which are easier to duplicate or clone if they are unpackaged, create unprecedented (but foreseeable) risks for an end-user: (a) attackers can gain access to their accounts, calls, text messages and credit card details; (b) there is an increased real risk of identity theft; (c) financial loss from unauthorised transactions; (d) privacy invasion and extortion; (e) the disruption of trusted communication services; and (f) loss of personal information.

[16] See further media reports here and here.

20.3. **Third**, it does not facilitate the adequate monitoring and containing of AML risks and compliance with global AML/CTF policies.

20.3.1. With the proliferation of unpackaged pre-RICA'd SIM cards, there is the obvious and direct risk of increased criminal, money-laundering, and terrorist activity, and the concomitant impact on law enforcement's ability to combat these crimes.

20.3.2. However, the inability to trace and combat money laundering and terrorist activities has also indirectly affected the South African public and its economy through the country's recent grey-listing by the Financial Action Task Force (**FATF**).[17]

20.3.3. The FATF regards South Africa as a jurisdiction as having "*strategic deficiencies in* [its] *AML/CFT regimes that pose significant threats to the financial system of the EU*". FATF has recommended that South Africa should work to improve its existing AML regime by, *inter alia*:

20.3.3.1. improving risk-based supervision of **designated non-financial businesses** and professions, and demonstrating that all AML/CFT supervisors apply proportionate and effective sanctions for noncompliance;

20.3.3.2. **ensuring that competent authorities have timely access to accurate and up-to-date beneficial ownership information on legal persons and arrangements**, and applying sanctions for breaches of violation by legal persons to beneficial ownership obligations;

20.3.3.3. **demonstrating a sustained increase in law enforcement agencies' requests for financial intelligence from the Financial Intelligence Centre** for its money laundering/terrorism financing investigations;

20.3.3.4. **demonstrating a sustained increase in investigations and prosecutions of serious and complex money laundering and the full range of terrorism financing activities** in line with its risk profile;

20.3.3.5. **enhancing its identification, seizure and confiscation of proceeds and instrumentalities of a wider range of predicate crimes**, in line with its risk profile; AND

20.3.3.6. ensuring the effective implementation of targeted financial sanctions and **demonstrating an effective mechanism to identify individuals and entities** that meet the criteria for domestic designation.

20.3.4. The FATF Recommendations arguably capture the deficiencies with RICA that have been set out in this submission. More importantly, they are reflective of the well-documented inadequacies of South Africa's AML, CTF and law enforcement capabilities, which have now caused the country's opprobrium by global watchdogs.

20.3.5. The censure by FATF is not helped by the coverage in the media of the deficiencies in RICA as highlighted above.

[17] The FATF Grey List is a list published by the Financial Action Task Force, i.e. the FATF, in which jurisdictions identified as having strategic Anti- Money Laundering and Countering the Financing of Terrorism deficiencies.

20.4. **Fourth**, the proliferation of unregistered SIM-cards in such significant numbers as described in this submission could have the contrary, yet equally perverse, effect of inadvertently extending the State's surveillance capabilities, which is contrary to the purport of the *AmaBhungane* judgment. This is so in that:

20.4.1. an exemption under RICA has been gazetted, in terms of which police are permitted to own advanced and otherwise illegal surveillance equipment, such as:

20.4.1.1. international mobile subscriber identity-catcher or "*IMSI-catchers*";

20.4.1.2. equipment reasonably necessary to be used with such IMSI-catchers;

20.4.1.3. software to be installed on such IMSI-catchers or equipment reasonably necessary to be used with such IMSI-catchers; and

20.4.1.4. various other forms of surveillance equipment;

20.4.2. the aforesaid equipment will enable police intercept the mobile phone traffic and tracking location data of mobile phone users in a manner which is subversive to South African's constitutional right to privacy to ordinary civil liberties and values;

20.4.3. the mass proliferation of SIM-cards on an unregistered basis exposes a significant number of end-users to interception of their mobile telephone communications, whether through use of registered or unregistered SIM-cards; and

20.4.4. since the mass proliferation of unregistered or pre-RICA'd SIM-cards effectively opens the door for the State to conduct large-scale surveillance on the unsuspecting public, the provisions of RICA are at odds with the findings of the Constitutional Court in *AmaBhungane*, which findings seek to protect and uphold the right to privacy.

E. Recommendations

21. Our view is that there is a simple solution to addressing the loopholes and inherent weakness in RICA. This solution is the distribution of SIM-cards in such a way that:

21.1. unique identifier information on a given SIM-card (e.g. MSISDN-numbers, ICCID-numbers, PUK and PIN numbers) is concealed so that it is not visible to the naked eye nor discernible by manipulation of the underlying packaging;

21.2. in tamper-proof (or tamper-evident or tamper-resistant) packaging, preventing counterfeiting, the duplication and/or cloning of the underlying SIM-card, and in a manner that protects SIM-cards and SIM-card related information (much like the distribution of bank cards), the packaging of which ought to be undertaken;

21.2.1. in the Republic of South Africa;

21.2.2. at a facility that complies with international quality management standards such as, for example, ISO 9001;[18]

[18] ISO 9001 refers to a set of quality management standards set by the International Organisation for Standardisation.

21.2.3. subject to appropriate data encryption and management systems whereby sensitive ICCID and PUK dated is encrypted during transmission, storage and production, by way of appropriate measures;

21.2.4. subject to appropriate product specifications; and

21.2.5. by and on behalf of / for the benefit of appropriately accredited vendors and service providers.

21.3. This solution can be easily effected into the Bill, or by way of draft regulations for public comment. In order to effect this solution, our recommendations are that the Bill be amended to:

21.3.1. include as one of the objects of the Bill, measures to address the proliferation of unregistered or non-compliant SIM-cards and SIM-card-related information;

21.3.2. either by further amendment or through regulation, augment section 40 of RICA by the adoption of protection and security related measures of SIM-card related information, which may be achieved through packaging or other means;

21.3.3. impose the obligation for such measures on the MNO responsible for the distribution and later, the registration and activation of SIM-cards;

21.3.4. establish a list of specifications under which pre-paid SIM-cards and related information ought to be protected and packaged, which methods may include:

21.3.4.1. tamper-evident, tamper-resistant or tamper-proof packaging;

21.3.4.2. disclaimers on the outside of the packaging that a SIM-card will not activate until the customer's RICA registration has taken place;

21.3.4.3. disclaimers on the outside of the packaging that the customer ought not to accept the SIM-card if the seal / packaging has been opened or there is evidence of tampering;

21.3.4.4. that SIM-cards be affixed / placed within packaging in a manner that prevents disclosure of MSISDN- and ICCID-numbers (while barcodes, SKUs, or other numeric coding schemes may be included on the outside of the package for inventory or activation purposes);

21.3.4.5. MNOs' terms and conditions ought to be within packaging by way of the use of appropriate collateral materials, which terms must set out the consequences of using a pre-RICA'd SIM-card; and

21.3.4.6. instructions for SIM-card activation, and usage and acceptance information;

21.3.5. the provision of specific penalties for non-compliance with section 40 in the form of criminal sanctions and higher thresholds for fines than those currently contemplated for non-compliance with section 40 of RICA.

22. PISA further recommends that these recommendations and this submission be considered by the Minister and the Committee in consultation with the Cabinet Minister responsible for communications, and that the appropriate regulations be put in place in accordance with section 40(4)(b) to the extent required to give effect to any of these recommendations should the Minister deem it appropriate to do so.

F. Conclusion

23. PISA would like to thank the Committee for affording it the opportunity to present its submission on the Bill. We trust that this submission will be received by the Committee in the spirit with which it is intended, and that the Committee will appreciate the relevance of PISA's concerns with the current legislative framework as set out above.

24. To this end, PISA is available to address any questions that the Committee may have and would welcome any opportunity to contribute and assist the Committee both in the formulation and finalisation of the proposed amendments.

G. Request to make oral submissions to the Committee

25. In addition to this written submission, PISA asks for an opportunity to make oral submissions to the Committee on the Bill, arising from the issues set out in this submission. This opportunity will allow PISA to field any questions that the Committee may have and to present on specific issues of interest and of relevance to the Committee.