Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

20th July 2017

The Portfolio Committee on
Justice & Correctional Services

Attention: Mr V Ramano **Per email: vramano@parliament.gov.za**

Dear Sir,

RE: SUBMISSION IN RESPECT OF THE CYBERCRIMES AND CYBERSECURITY BILL ("the Bill") FROM THE CREDIT BUREAU ASSOCIATION

We have been advised that final submissions to the amended Bill can be made to your offices on or before 28th July 2017, and accordingly, the Credit Bureau Association ("the CBA") hereby provides its comments to the Bill.

1. Background

The CBA is a voluntary body that promotes fair and equitable services in as far as credit bureau data is concerned. It ensures the confidentiality, accuracy, relevancy and utilisation of data in accordance with international best practice and relevant legislation. The CBA's mandate is to provide a framework for a sustainable and well-functioning credit information system by facilitating fair practice within the credit bureau industry as well as promoting transparency, accountability, high quality credit reporting and sound business practices.

The CBA currently represents 10 of the 14 registered credit bureaux in South Africa, being five full members who hold consumer credit information (Compuscan, Consumer Profile Bureau, Experian, TransUnion and XDS) and five associate members (Cred-IT Data, Inoxico, Lexis Nexis Risk Management, Vericred and TPN Credit Bureau).

Credit bureaux are privately owned and independent organisations that receive, compile and maintain information from credit providers, data suppliers and other (private and public) sources regarding a consumer's credit history and payment behaviour. Credit bureaus compile and issue credit reports for the purposes permitted or required in terms of the National Credit Act, 34 of 2005, and its Regulations thereto, as amended from time to time ("the National Credit Act").

Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

2. Submission by members of the Credit Bureau Association in respect of the Bill

2.1. Classification as a National Critical Information Infrastructure

2.1.1. The CBA has been informed that one of foundational documents for the Bill is the National Critical Information Infrastructure Policy. It is not clear whether this is in a draft form or whether it has been finalised and remains classified. Either way we are advised that the policy is not available. This makes it extremely difficult to comment properly on these provisions, but in good faith the CBA shall attempt to do so.

2.1.2. In terms of the Bill, the Minister of State Security is granted the power to declare any information infrastructure, or category or class of information infrastructure or any part thereof as a National Critical Information Infrastructure ("NCII"), including where it appears that an information infrastructure is so important that any interference with, loss or damage thereto may "cause major economic loss", or cause "destabilization of the economy". The extremely vague and wide wording of "any major economic loss" is a further concern. In the first instance, it does not indicate to whom major economic loss may be caused. Simply by not being able to access credit as a result of credit information being defective, an individual may suffer major economic loss to the individual. This is cannot be intended in the context of a credit bureau and it is more likely that major economic loss refers to economic loss in a National context. Similarly, the wording "destabilization of the economy" is purely within the discretion of the Minister of State Security. While a check is provided in sub-section 3, this places a fairly onerous burden on any company that might be subjected to the Minister of State Security's decision in this regard. It also does not currently allow for companies to be represented by a representative body such as the CBA. This may mean that all of the members of the CBA would have to individually appeal a declaration by the Minister of State Security declaring information infrastructure to be a nationally critical information infrastructure.

2.1.3. An information infrastructure that is declared to be a NCII must comply with regulations promulgated in terms of section 58(5) – these include amongst others, the Minister making regulations regulating (i) policies and procedures to be applied to NCIIs; (ii) access; (iii) storing, archiving of information; and (iv) minimum physical and technical security measures to be implemented to protect the NCII.

2.1.4. Credit bureaux are regulated by the National Credit Regulator and are required to comply with all of the applicable sections of the National Credit Act 34 of 2005 ("NCA").

2.1.5. Section 68 of the NCA, stipulates the circumstances in which a report containing confidential information belonging to a consumer can be released or reported. Credit bureaux are further obliged to ensure that the confidentiality of data is maintained and that all relevant legislation regarding privacy and confidentiality of information is adhered to.

Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

2.1.6. Upon commencement of the Protection of Personal Information Act ("POPIA"), credit bureaux, being processors of personal information, will also be regulated by the Information Regulator, resulting in credit bureaux being regulated by two regulators. In terms of POPIA, codes of conduct may be issued by the Regulator. These codes are intended to be specific to "specified industry, profession, ... class of industries, professions...". It is submitted that codes of conduct governing specified industries or professions, which in terms of POPIA must establish the granularity relating to compliance with the conditions of lawful processing of POPIA, including the security safeguards required in terms of sections 19 and 22 of POPIA, will be far more appropriate than general minimum information security guidelines contemplated in the Bill.

2.1.7. As previously indicated, the credit bureau industry in South Africa is highly competitive, with little risk of credit bureau services and information becoming totally lost, damaged, disrupted or just unavailable to the South African business and financial sectors. In addition, each credit bureau has their own disaster recovery and business continuity programmes in place, should an adverse event or disaster occur. If codes of conduct are established as contemplated in POPIA, the generally acceptable information security practices referred in POPIA will be interpreted by the Information Regulator to ensure appropriateness in respect of the Credit industry, as has been the case in other jurisdictions.

2.1.8. Credit bureaux who have international parent companies are also subject to their global information security policies implemented and rolled out by their parent companies. The policies are based on international data protection (privacy laws that establish materially similar safeguards as are contemplated in Chapter 3 of POPIA) and data security laws and international best practice standards. In this regard, these credit bureaus have over the years heavily invested in resources, including financial and technical measures, controls and people, in order to secure the information.

2.1.9. The definition of "critical data" is too broad and includes "the personal affairs of any person" and "commercial information that could cause undue advantage or disadvantage to any person". Credit bureaux hold commercial information on data subjects and such over-broad definitions has the potential to lead to legislative overkill and abuse for ulterior motives.

2.1.10. For the reasons outlined above, members of the CBA submit that credit bureaux be specifically excluded from the definition of an NCII, or be exempted from being declared an NCII.

2.1.11. It is agreed that information is not always processed within defined silos and that information may very well be exchanged between a structure that is a NCII and one which is not. Where a cybercrime is committed affecting such data, cooperation by both entities will be required – irrespective of whether it is a NCII or not.

Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

Exclusion from the definition as highlighted in 2.1.10 above will not prevent a credit bureau from engaging and fully cooperating with the applicable law enforcement agencies in the event of such a cybercrime or similar offence being experienced.

2.2. Electronic Communication Service Provider

2.2.1. The definition of an Electronic Communications Service Provider ('ECSP') is currently so broad and it has the unintended consequence of including registered credit bureaux to be subject to all provisions applicable to ECSPs. See 2.2.3 below.

2.2.2. In this regard, credit bureaux transmit, receive, process and store data and information sourced from the various data suppliers who without limitation, include electronic communication services (e.g. mobile network companies and telecommunications providers), as well as those data suppliers who are financial institutions (e.g. banks, insurers, etc.) and other persons.

2.2.3. Part c(ii) of the definition of ECSP's includes those entities who transmit, receive, process or store data of any person and by virtue thereof all such entities will be subject to the obligations set out for ECSP's.

2.2.4. A further observation is that if the Bill is passed as is, and without carve outs or safe harbours, by virtue of the definition of ESCP's it will, by way of example, include employers that process or store employee data, any retailer (both virtual and physical) that processes a purchaser's credit card information, or any website that stores its visitors' cookie data, even if only temporarily.

2.2.5. Section 64, under the heading of 'General obligations of ECSP's and liability', places obligations on ECSP's to :

a) take reasonable steps to inform its clients of cybercrime trends, which affect or may affect the clients of such an electronic communications service provider;

b) establish procedures for its clients to report cybercrimes with the electronic communications service provider;

c) inform its clients of measures which a client may take in order to safeguard himself or herself against cybercrime.

2.2.6. The obligations, as provided for in section 64(1), insofar as credit bureaux are concerned, are most likely to have very little effect.

Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

Rather, we wish to draw your attention to certain obligations placed on parties processing personal information in terms of POPIA (including credit bureaux), namely, to notify the Information Regulator in the event of a data subjects' personal information being accessed by an unauthorised person, and which is required to be made 'as soon as reasonably possible after the discovery of the compromise taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope for the compromise and to restore the integrity of the Responsible Party's information systems'.

2.2.7. It should be emphasised that having independent regulation, as is contemplated in POPIA, in dealing with a breach of personal information, is preferable. Firstly, it allows for an independent party to deal with and establish whether appropriate mechanisms for dealing with compromises are established. Furthermore, the onerous obligations placed on ECSPs cannot be undertaken by credit bureaux. This would mean an extension of the normal and accepted information security practices that should be established and maintained by credit bureaux and it cannot be reasonably expected of every ECSP, particularly with the wide definition as it currently stands, to establish the capability to inform on cybercrime trends or measures that are necessary to guard against cybercrimes.

2.2.8. Similarly, the provisions of Condition 7 (sections 19 – 22) of POPIA places onerous obligations on all responsible parties to ensure security safeguards, whilst section 22 requires notification of security compromises to the Information Regulator and the affected data subject/s and methods to be established to protect the affected data subject/s. The notification to a data subject in this instance, may only be delayed if a public body responsible for the protection, detection or investigation or the Information Regulator determines that the notification will impede the criminal investigation.

2.2.9. The provisions of section 64(2) and section 64(3) of the Bill may pose a challenge to credit bureaux and we propose that credit bureaux at best be required, on a voluntary basis as opposed to being mandatory, to comply with section 64(2). As previously stated, credit bureaux are required in terms of POPIA to report any security compromises to the Information Regulator.

2.2.10. Assuming that credit bureaux are defined to be ECSPs and are not specifically excluded from the provisions of the Bill, additional financial burdens on credit bureaux, which will simply be passed on to credit bureau clients who in turn may pass the cost on to data subjects (including individuals and entities) resulting in the cost of credit yet again being increased, to meet these additional regulatory obligations. As the Bill has not been aligned with the provisions of POPIA, which is in alignment to meet the constitutional right to privacy, the obligations of credit bureaux would be duplicated and in certain instances be incompatible with one another. This would create an unnecessary financial burden for credit bureaux who already have to comply with data security obligations imposed by the NCA and POPIA.

Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

2.2.11. Against this background, it appears unnecessary and unreasonable for credit bureaux to have to report data compromises to multiple regulatory bodies. It is submitted that in any event the Information Regulator would, if both bodies are to perform their functions properly, forge a strong liaison with appropriate law enforcement bodies to ensure that information is communicated between the parties that may be necessary. Therefore, it seems far more appropriate, feasible and preferable for credit bureaux to report a security breach to the Information Regulator (as already provided for in POPIA) who in turn could engage the national cybercrimes centre or other law enforcement agency/ies as may be relevant given the circumstances.

2.2.12. We propose that credit bureaux be specifically excluded from the definition of ECSPs, or alternatively, be exempted from mandatory compliance to the provision of sections 64(2), 64(3) and 64(4).

2.3. Capacity of the judiciary and law enforcement services to perform responsibilities in terms of Bill

2.3.1. The Bill, in its current form, provides for the judiciary to issue warrants and to give certain 'instructions' in as far as the treatment of an article in the case of a breach or suspected breach is concerned. An article may be data, a computer network, a database and the likes).

2.3.2. Similarly, law enforcement officers may, amongst other things, enter, access and seize any article on the basis of a verbal warrant. Verbal warrants would be difficult to prove and the power given to the law enforcement officers to act on verbal warrants could well lead to abuse and confusion.

2.3.3. This gives rise to concern as the data and infrastructure required by credit bureaux to receive, process and host data is highly sophisticated and will require a sophisticated level of understanding to ensure that these processes are correctly executed.

2.3.4. Furthermore, this may infringe a person's constitutional and other legal rights to privacy, and well as credit bureaux' duty to keep confidential information secure.

2.3.5. A further concern has been raised with government by a number of commentators, being the lack of capacity, professional skill and competence within the SAPS and the National Prosecuting Authority to deal with cybercrimes. It is respectfully submitted that unless this capacity and competence is created the aims of the Bill will not be achieved. While the Bill peripherally refers to capacity building, it is submitted that it will be necessary for the credit industry to work with government and regulators to allow the relevant authorities the opportunity to gain an understanding of the credit industry, the wide base of information that is used in establishing appropriate South African centric credit information, as well as measures necessary to secure the information. As it stands the Bill does not allow for the proper establishment of a public/private partnership of this nature. See further comment in 2.5 below.

Credit Bureau Association
St Georges Park, The Oval Office Park, 1 Meadowbrook Lane, Bryanston
PO Box 2146, Pinegowrie, 2123
T 011 463 8218 | E enquiries@cba.co.za
W www.cba.co.za

cba credit bureau association

2.4. Penalties

Oversight by three different regulators may additionally result in an overlap, not only in as far as obligations are concerned, but also in terms of possible penalties and fines being imposed for the same offense. The jurisdictions of the various regulating entities would need to be clearly defined.

2.5. Private Sector partnerships

The Bill, in its current form, places onerous obligations on the private sector to, at its own cost, establish Private Sector Security Incident Response Teams. Although we encourage engagement and stress the creation of public/private partnerships, the current requirements merely create onerous and costly obligations for the private sector.

We look forward to further engagement in this regard.

Yours sincerely,

Alison Magrath

CBA Executive Manager