BANKSERVAFRICA

Parliamentary Submission – FIC Amendment Bill

December 2015

PO Box 62443, Marshalltown, 2107
Tel: +27 11 497 4000 / Fax: +27 11 493 0595

Dear Mr Allen Wicomb,

Standing Committee on Finance: BankservAfrica FICA Solution enables the effective implementation of the proposed amendments under the FIC Amendment Bill

The South African Bankers Services Company (Proprietary) Limited ("BankservAfrica"), intends to enhance the effectiveness and efficiency of compliance requirements applicable to all accountable institutions ("AIs") in terms of the Financial Intelligence Centre Act 38 of 2001 ("FICA"). As a result, BankservAfrica would like to present the BankservAfrica FICA Solution ("BFS") to the Standing Committee on Finance ("the Committee") in order to advise the committee on the manner in which the abovementioned solution supports and enables the effective implementation of the changes proposed in the Financial Intelligence Centre Amendment Bill of 2015 ("the Bill").

The aim of our submission and subsequent proposed presentation to the Committee by Max Sokolich and Martin Grunewald is to present the proposed solution and the status of project. The project thus far has been supported by an Industry Steering Committee which has had active participation and support from National Treasury (Chair), Financial Intelligence Centre (FIC), Association for Savings and Investment South Africa (ASISA), Banking Association of South Africa (BASA), BankservAfrica and the Johannesburg Stock Exchange(JSE).

Executive Summary

BankservAfrica play a key role in the South African financial services sector. Currently, they provide stability to the National Payment System. This service ensures that transaction processing and settlement in South Africa takes place quickly and efficiently. As a result, BankservAfrica is seen as a trusted service provider.

The provider and operator of a FICA Solution should be reliable in managing large volumes of data, securely. BankservAfrica are in a unique position to offer a service of this nature. The reason for this, is that BankservAfrica, is owned and controlled by the banking industry and currently are entrusted by the banking industry to provide secure, reliable and trusted payment and settlement services.

BankservAfrica is authorised by PASA (Payment Association of South Africa) to act as a PSO (payment clearing house system operator) in terms of guidelines approved by SARB (South African Reserve Bank). SARB or the South African Reserve Bank is the central bank of South Africa and plays a pivotal role in ensuring financial stability and regulates South Africa's National Payment System and thus would ensure that the solution is operated within a regulatory framework.

During 2015 BankservAfrica undertook to develop a business case for the BankservAfrica FICA Solution ("BFS"). The process of developing a business case involved over thirty Accountable Institutions (AIs) who took part in over ninety hours of workshops. Based on the outcomes of the AI and FIC requirements workshops, the initial concept was adapted and culminated in the Business Requirements Specification (BRS) which was signed off by the Industry Steering Committee.

A number of key design principles were developed to ensure a solution that would be sufficiently robust and provide a number of benefits to the industry. These key design principles and benefits were further supported through the publication of the Bill on the 9th October 2015. The BFS provides a comprehensive solution which will enable an AI to adequately comply with the new requirements as stipulated in the Bill, particularly those that relate to, the screening of Domestic Prominent Influential Persons, Foreign Prominent Public Officials, verification of the Ultimate Beneficial Owners and it will assist an AI in their reporting obligations in that it will provide evidence of verification through the use of the audit trail.

It is therefore as a result of the above that BankservAfrica would like to present the full solution and support of the Bill to the Standing Committee on Finance.

Background

In 2006, an enquiry into aspects of competition in retail banking in South Africa (the Banking Enquiry) was initiated by the Competition Commission of South Africa and resulted in a set of recommendations released in 2008 (the Banking Enquiry Report).

There were 28 recommendations, with Recommendation 27 proposing the use of a central FIC Act hub which could be used to facilitate compliance with the FIC Act and making switching easier for bank customers. The recommendation asked National Treasury to pursue the establishment of a FIC Act hub.

The concept was essentially to perform the requirements under the FIC Act once and then re-use the verified data multiple times, with AIs sharing verified customer data via a centralised facility. At that stage, the idea was abandoned due to the perceived costs associated with such a facility, as well as the unresolved issues around liability should an AI act on the information verified by another AI.

In 2013 the concept was revisited and BankservAfrica board of directors, under the chairmanship of Manne Dipico, approved a project for BankservAfrica to investigate the concept of a BFS that could address the needs of all AIs in South Africa. BankservAfrica is wholly owned by 11 South African banks, which are represented on the BankservAfrica board of directors

Through the process of investigating the business case, the concept was explored and the business requirements were analysed, prioritised and described. This process resulted in changes to the scope of the original concept and the business case focuses on a subset of the original requirements.

The high costs associated with Know Your Customer ("KYC") include the time and effort involved in obtaining information and documents from customers, inability to effectively verify information provided, cost of penalties for non-compliance, cost of training and the cost of remediation. It is believed that there is an opportunity to decrease the costs associated with KYC.

The risk impacts include the ineffective nature of verification processes resulting in the onboarding of non-compliant customers (for example, through the use of fraudulent documents), risk of inadvertently facilitating money laundering, inability to retrieve evidence of verification performed during inspections and reputational risks. An opportunity exists to decrease the risk impacts for AIs.

The customer experience impacts include financial exclusion through being unable to provide requested documentation and the cost of compliance driving up the cost of the products, inconvenience and frustration which is contributed to by the lack of understanding of KYC. The opportunity exists to improve the overall customer experience.

BankservAfrica Business Objectives

The long term vision (2030) is to simplify the BankservAfrica "worlds" by combining trusted transactions with sensitive information. The BFS delivers on this vision by dealing with sensitive personal information and creating trusted transactions to support KYC.

BankservAfrica aims to create compelling value propositions for both shareholders and BankservAfrica clients. The value proposition will deliver three strategic pillars for 2015-2018. These pillars are as follows:

1. **Focus on role in the National Payment System (NPS):** Affirmation of BankservAfrica focus and priority on the highest level processing of clearing and settlement payments transactions in South Africa, ensuring the safety and stability of the NPS
2. **Stabilise processes:** Stabilisation and embedding of all key processes
3. **Client driven value-adds:** Ensuring BankservAfrica' s long term relevance and sustainability by extending the range of value-add services that fall within the scope of the shareholder memorandum of incorporation

The BFS supports the value-add pillar through the extension of the services offered to BankservAfrica clients. The BFS is a strategic initiative that leverages both current and new relationships to realise economies of scale. The BFS will ultimately drive efficiency across various industries. By adding diverse product offerings to a broader range of markets, the BankservAfrica footprint is extended beyond the financial services industry, thereby ensuring sustainability. The BFS aligns to the strategy to follow and support BankservAfrica shareholders into the rest of Africa.

Good corporate governance is fundamental to the integrity of BankservAfrica and the ability to manage risk and perform at optimum levels. BankservAfrica has an enterprise-wide risk management strategy, maintaining its focus on operational, regulatory compliance and information security risks. The BFS will enhance industry risk mitigation capabilities for BankservAfrica clients and will enable its clients to achieve regulatory compliance.

To retain its reputation, and to maintain its leading position in the industry, BankservAfrica employs world-class systems, infrastructure and expertise. The BFS aligns to this strategic intent.

In September 2014 when the Strategic BFS business case was submitted to the BankservAfrica board of directors for approval, the alignment to the BankservAfrica strategy included the following:

- Supplying the banking market with products – this is achieved more broadly by appealing to market segments outside of the banking industry
- Economies of scale through large volumes – this is achieved through creating a solution that covers large volume banks, small volume banks and other AI types that are not currently served by BankservAfrica
- Mitigating risks across the industry – the implementation of a BFS will enable participants to reduce risks for both the businesses and the industry as a whole
- Driving efficiency across the industry – the BFS enables efficiency within multiple industries that are currently impacted by the FIC Act
- Hosting and managing sensitive information – by hosting and operating the BFS, BankservAfrica, who is already a trusted partner can further existing relationships and the development of new trust relationships
- Applying standards across the industry - although this was the intent, the agreed design principles do not allow for this. The solution will allow each AI to subscribe to offerings and data providers and this will optimise standard approach within the internal AI environment

Why BankservAfrica?

BankservAfrica is an automated clearing house that has a forty year track record in the provision of interbank electronic transaction switching and settlement services to the South African banking and corporate sector as well as to some of the banks in Africa. BankservAfrica is regarded as a trusted, stable and sustainable service partner in the provision of high quality transactions, switching and value-added services.

BankservAfrica focuses on electronic clearing and settlement, outsourcing and facilitation of distribution infrastructure, replication of core competencies in other industries and intellectual property licensing, operations and consulting. These offerings are differentiated through the integration of value-added services and exceptional service levels, coupled with competitive and stable prices.

Core services means the clearing services that BankservAfrica performs as a Payments System Operator on behalf of a Payments Clearing House participant. Any other services intricately linked to a Payments Clearing House and/or which substantially assist in reducing risk to the NPS shall

be included as Core Services from time to time. The regulation of these core services falls under the ambit of the SARB.

BankservAfrica clients are assured of the highest quality transaction, switching and value-added services in support of the business objectives; while effecting significant cost savings through economies of scale and minimising risk and complexity in the industry.

By leveraging infrastructure, BankservAfrica is able to support emerging and developed payment environments. The multiple electronic delivery capabilities facilitate connectivity, message management, billing and compilation of management information.

BankservAfrica's core capabilities centre on enabling interoperability across multiple participants over multiple payments types, reducing risk and complexity in the respective payment systems.

Based on the principle of inter-operability between clients to facilitate payment transactions, BankservAfrica encourages and facilitates interagency cooperation within the industry. BankservAfrica value trusted and stable relationships with industry regulators and the maintenance of these relationships are important.

Objectives of the BFS

The goal of the BFS is to improve counter money laundering capabilities and ensure compliance with legislation, whilst simplifying the FICA processes for all stakeholders. This goal supports the National Policy of improved access to financial services and the regulatory objective of effective and efficient adherence to the FIC Act.

Specific objectives which will be achieved are as follows:

- Reduce time required to KYC customers
- Increase the accessibility of data to enable verification of customer information
- Decrease the cost of verifying customer information
- Enhance the customer's KYC experience
- More effective means to prevent customers with a propensity to commit fraud / money-laundering from entering into / remaining in the system
- More efficient and effective means for AIs to comply with the KYC obligations under the FIC Act
- Minimise impact of regulatory change, through having a single integration point.
- Increased financial inclusion, through the Reduced reliance on paper evidence of verification for KYC purposes

Due to the extensive regulatory environment a number of key principles needed to be defined upfront in order that the design of the solution would be legal. These key principles are:

- Compliance obligations under the FIC Act provide the basis upon which the BFS must be designed
- Responsibility and accountability for compliance with the provisions of the FIC Act remain with the respective AI
- The BFS will not become an accountable or reporting institution (as defined in the FIC Act)
- Only trusted and credible data sources will be used as Data Providers
- The FIC must have unfettered access to the complete set of information created and maintained by the BFS
- The BFS must seek to minimise the negative impact on customers and should not lead to an increase in costs for the customer
- The BFS should support all types of AIs and should result in cost efficiencies across the industry
- Notifications based on trusted Data Provider information and previously verified information, are allowable if the relevant customer consent has been put in place
- A customer may not have direct access to the BFS
- Only AIs that have been registered with the FIC will be granted access to the BFS
- The BFS shall support all types of customers
- BFS subscribers may opt-in and out of service usage
- Verification enabled against data
- BFS shall drive cost efficiency for stakeholders

As part of the solution design a number of exclusions were also considered. These included:

- The BFS will not perform transaction monitoring such as Suspicious Transaction Reporting (STR) and Cash Threshold Reporting (CTR)
- The BFS will not serve as a central store of customer KYC data on behalf of the AI
- The BFS is specifically not intended to be a document or content management solution
- The BFS will not be accessed directly by AI customers
- The BFS will not maintain a FIC Act status for a customer

Solution Summary

The BFS will offer subscribers the following services through a single integration point:

- Validation service
- Notification service
- Screening service
- Adverse media service
- Customer enquiry service

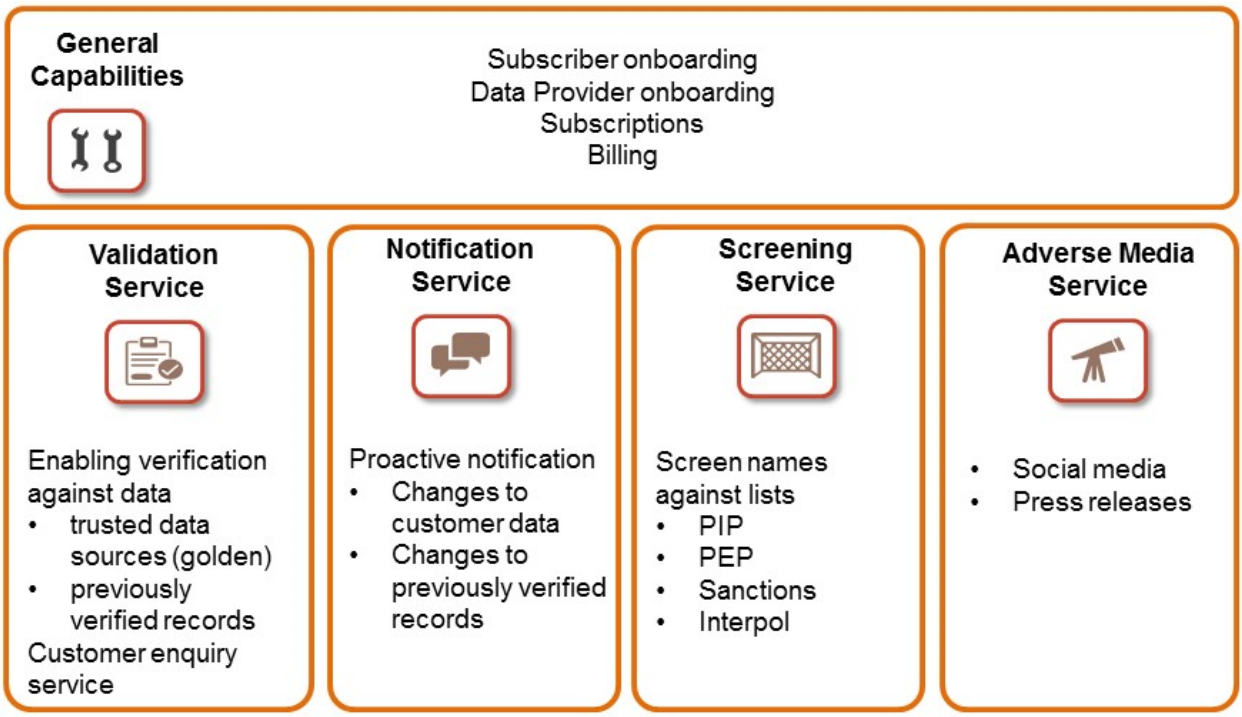

Figure 1: BFS Summary of Services

The simplest example of a validation service is as follows:

- A customer (SA resident) applies for a new banking product and identifies themselves to the bank representative using a South African ID document or biometric and supplies requested information. (No documentation is required)
- The bank representative captures the information provided by the customer. This information is then submitted to the BFS. An audit trail is created for this submission.
- The BFS retrieves requested information from data providers. The information is then presented to the bank representative. An audit trail is created for the validation response.
- The bank representative confirms that the information provided by the customer is the same as the information supplied by the data provider. An audit trail is created to record the AI verification confirmation.

An example of a validation service which re-uses previous validation responses and/or verification selections is as follows

- The same customer (SA resident) applies for a new banking product at another accountable institution within a 3 month period. (No documentation is required)
- The bank representative captures the information provided by the customer and submits the details to the BFS. An audit trail is created for the validation request.
- The BFS retrieves previous validation responses and/or verification confirmations for the same customer (for the same information request) from the audit trail. (In this case, no additional information is retrieved from a data provider which results in efficiencies and cost savings). The information is presented to the bank representative and an audit trail is created for the validation response.
- The bank representative confirms that the information provided by the customer is the same as the information supplied by the BFS. An audit trail is created for the verification confirmation.

The option will exist for the AIs to subscribe to data providers and/or previous validation responses and/or previous verification confirmations, with configurable parameters such as the age of the previous audit trail.

A more detailed description of the end-to-end solution is described below with the associated diagram.

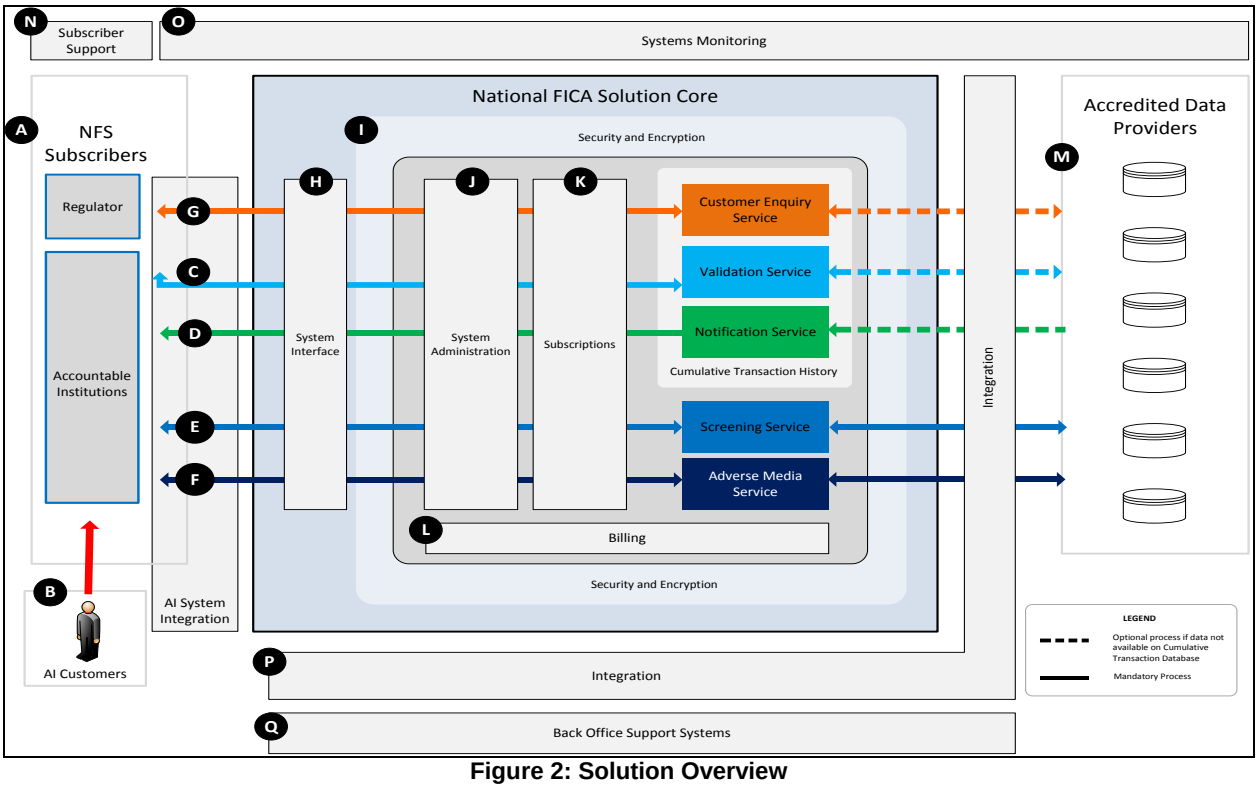

Figure 2: Solution Overview

Solution Description

Key role players, BFS services and interactions are described below.

The **BFS subscribers (A)** include the regulator (FIC), any other institution registered with the FIC, or regulatory bodies authorised by the FIC to use the solution. These include AIs as listed in the FIC Act.

The **AI customer (B)** is the person or entity with whom an AI has a business relationship and requires validation and verification for KYC purposes.

Subscribers will be able to register for available services and customise the subscriptions. Any and all interactions with the BFS will be recorded into an audit trail. For validation and notification services the customisation can occur at the level of specific data attributes. For illustrative purposes, an example is presented to describe how each of these services may be utilised.

The **validation service (C)** will involve the submission of customer data to selected data providers in the form of a validation request. Information will be returned to the subscriber, in the form of a validation response. The validation response will provide a data set in response to the original request, not in the form of a “yes” or “no” response, but rather a set of data sourced from the various data providers (as selected by the subscriber) based on the type of data categories requested. This may enable the subscriber to perform the verification obligation set out in the FIC Act. The selection and confirmation of a validation response by the subscriber will result in the creation of a verification record.

For the validation and notification services, a match percentage which is configurable per subscriber will be applied to the service responses. This allows the subscriber to only receive information from data providers within a selected match range such that a practical number of service responses are returned. This may enable a more efficient verification process.

An example of the validation service could be the validation of a trust. Information about the trust (provided by the subscriber’s customer) would be submitted by the subscriber user to the BFS. The trust information would be requested from the data provider/s (selected during service subscription), for validation. The information on record at the data provider/s would be received by the BFS and matching rules (as defined in the service subscription) will be applied and the results presented back to the subscriber user. This puts the subscriber user in a position to make a decision around verification of trust information. The subscriber user may select the most appropriate validation result as the verification selection.

The subscribers may also elect to perform the validation services against previous verification records and validation responses within a specified period.

Using the example above, the trust information provided by the subscriber's customer would not be requested from the data provider/s but rather from recent validation requests or verified records within the BFS.

The **notification service (D)** is based on trigger events such as:

- A change was identified for a previously verified customer record at the data provider.
- Any other subscriber selects a different validation response option, for the same validation request, from the last verified customer record. In this case, other subscribers who selected the previous verified record will be notified of the change.

Subscribers can customise the notification subscription for specific trigger events and frequencies in order to accommodate risk based approach requirements.

In the case of the trust example, the subscriber may request to receive notifications should any information regarding the trust change within a defined period. The BFS will periodically scan the data provider/s, validated records and verified records and where change is identified, the subscriber will be notified of the change. This will enable the subscriber to re-validate the trust information.

The **screening service (E)** may provide subscribers with the ability to screen customers against a number of screening lists and a screening result is sent to the subscriber.

In the case of the trust example, Individual trustees / beneficiaries of the trust may be screened. The trustee / beneficiary information will be submitted to the BFS and this information will be compared to lists (such as sanction, Politically Exposed Persons and watch lists).

The **adverse media service (F)** may enable subscribers to obtain customer-specific media references. The response would comprise a report on unfavourable information found in a variety of referenced sources.

In the case of the trust example, where required, a subscriber may request an adverse media search to be performed on individual trustees / beneficiaries of the trust. The request for such searches will be submitted to the BFS and the back office administrator will perform the search for adverse media reporting. The report will be compiled and sent to the subscriber. This will enable the subscriber to make decisions that are in line with risk based approach.

The **customer enquiry service (G)** will only be accessible by the FIC. The FIC may request information on a specific customer or legal entity and all possible information available at selected data providers will be returned. The information will not be matched or filtered.

An example would be if FIC required additional information regarding a particular trust and / or trustees and beneficiaries, the FIC user would submit a request to the BFS. The information would be requested from the data provider/s (selected during service subscription). The information on record at the data provider/s would be received by the BFS and the result set presented to the FIC.

The provision of these services requires a number of supporting functions; these include take on of data providers, the creation of subscriber profiles and authorisation of users.

The **system interface (H)** will provide subscribers with mechanisms to interact with the BFS. Services will be accessed through web services (online service delivered through a website) and file transfer mechanisms.

Security and encryption (I) is intended to prevent unauthorised access to and hacking of the BFS through incoming and outgoing message encryption. The system administration, subscriptions and billing portions of the BFS are encompassed within this.

The **system administration (J)** function enables profile management, user account management and access control.

The **subscriptions (K)** will define the service offerings that each subscriber has registered to use.

The **billing (L)** component of the BFS will track service usage and facilitates the preparation of invoices.

Accredited data providers (M) are approved parties from whom data shall be sourced.

Adverse media data providers (N) supply published material, web based information and global news sources. Once sourced, the data will be utilised in order to enable service provision by the BFS.

Subscriber support (O) is the initial support level responsible for basic subscriber queries and escalations.

Systems Monitoring (P) will contain the technology components that will provide technical support personnel with a view of system performance issues and bottlenecks amongst other system health check monitoring capabilities.

The integration (Q) layer allows information exchange between the BFS and any external systems that the solution interacts with.

Back office support systems (R) include the enterprise resource planning application, the customer relationship management application and the service desk management application.

Solution Support for the FIC Amendment Bill

The Bill introduced a number of key changes in the customer due diligence requirements which are applicable to all AIs. The BFS provides support to AIs to implement the required amendments. A number of the key requirements under the Bill with the associated support which may be leveraged from the BFS are discussed below.

Domestic Prominent Influential Person and Foreign Prominent Public Official

Section 21F and 21G require an AI to identify whether a prospective client or the beneficial owner of the prospective client are a domestic prominent influential person or a foreign prominent public official. The AI will be responsible for performing ongoing enhanced due diligence. These requirements are further extended through the inclusion of *s* 21H, which requires that the above sections apply to the immediate family and known close associates of the domestic prominent influential person or a foreign prominent public official.

The BFS can assist an AI through its use of a number of data sources and in particular the **screening service** as described above to identify such individuals. This reliance can be placed on the utility due to one of the key principles defined above in the design of the solution that only credible data sources and data providers will be utilised.

Further, the **notification service** will also be able to inform the accountable institution of changes in a person's status. For example, a new Chief Executive Officer is appointed for the South African Post Office. In accordance with the definition of a domestic prominent influential person as included in *s*1 this person would need to be considered in terms of *s*21F. His / her children, spouse and parents etc. as defined by *s*21H would also fall within *s*21F. As a result, the **notification service** could inform the AI of this change in relationship and the AI will be in position to appropriately apply the requirements of sign-off and on-going due diligence.

Due to the anticipated cost savings and economies of scale to be achieved by the solution, small AIs would benefit from the BFS as they would be able to identify persons who fall within the requirements of *s*21, *s*21G and *s*21H of the Bill.

Persons and Entities Identified by Security Council of the United Nations

Section 26A requires that "*upon the adoption of a resolution by the Security Council of the United Nations under Chapter VII of the Charter of the United Nations, providing for financial sanctions which entail the identification of persons or entities against whom member states of the United Nations must take the actions specified in the resolution, the Minister must announce the adoption of the resolution by notice in the Gazette and other appropriate means of publication.*" The prohibitions placed on these individuals and entities are defined in *s*26B of the Bill.

The BFS can assist the AIs in the identification process through the use of two key services being the **notification service** and the **screening service**. The notification service can inform the AI of

the change in status of the previously verified individual. As only trusted data sources are utilised, these data sources will be updated to reflect the new United Nations requirements and these will filter through into the BFS. Further, any future screening requests required by the AI will update the verified record of the person or entity. An AI will then be provided the necessary information on which they will be able to make a decision on how to respond to a specific request.

Ultimate Beneficial Ownership

A key change to be implemented with the Bill is the requirement to identify and verify the Ultimate Beneficial Owner (UBO). Section 1 of the Act defines an UBO as *"in respect of a legal person, means a natural person who, independently or together with another person, directly or indirectly—*
(a) owns the legal person; or
(b) exercises effective control of the legal person;"

Section 21B requires an AI to identify and to take reasonable steps to verify the identity of the UBO of all legal persons, trusts and partnerships. The BFS can assist an AI in taking the reasonable steps to verify the identity of a UBO. This will be performed via the **validation service**. The AI will receive information from a number of data providers or from the previously verified audit trail record from the BFS. This will be confirmation of a verified record. As an UBO is at times removed from the entity, obtaining verification documentation may not be possible or practical. However, as the UBO's record has previously been verified by the BFS, the AI could rely on this record as reasonable steps undertaken to verify the UBO's identity. The manner in which the validation service operates would not place any obligation on the BFS to determine the client's UBO nor will the BFS store the information as a UBO.

The service, provided the client has provided the necessary consent, will assist an AI in verifying the details of the UBO. A good example of this is where a prospective client of an AI attempts to open up a bank account on behalf of a legal entity. This legal entity is owned through a complex group structure where the UBO may be six or seven layers removed from the client. The client may not be able to obtain a copy of the person's identity document, but does however, have information such as the name, surname and identity number of the person. The AI will be able to capture this information into the system and the validation service will return a recently validated entry for the client or information from a number of data sources. The AI will then be able to select the most relevant entry as described in the overview of the solution above.

Therefore the difficult nature of verifying UBOs will be reduced.

Doubts about veracity of previously obtained information

The underlying principles of the BFS supports the inclusion of *s*21D of the Bill. One of these principles is that the AI is responsible for the compliance of the customer. The information returned by the data providers will be presented to the AI who will be responsible for confirming the information and creating the audit trail of the verified record. Therefore, when the AI is reviewing the verified information in line with the requirements of *s*21D the AI will be in a position to

determine whether the information received is adequate. If not, the AI will be able to generate a new verified record for the customer.

Through this process of creating new verified entries in the audit trail the adequacy requirement as described by *s*21D could be presumable fulfilled. The process of verification and the associated audit trail is enhanced as one of the underlying principles of the BFS is that the information being returned is credible and is not accessible by a client.

Records may be kept in electronic form and by third parties and must be kept in the Republic

The changes to *s*24 as required by the Bill support the use of a utility such as the BFS. The records utilised for verification will be accessible by the FIC as described in the **customer enquiry service**. Further, the BFS as part of its design principles require that the AI remain responsible for the KYC of their customer and will not store information on behalf of the AI. The BFS solution will be housed in South Africa as BankservAfrica operations are South African based.

Powers of access by authorised representative to records in respect of reports required to be submitted to Centre

The insertion of *s* 27A of the Bill, has resulted in the FIC or an authorised representative of the FIC being granted access to any records kept by or on behalf of an accountable institution in terms of *s*22, *s*22A and *s*24. It is however important to note that this access will only be granted to the FIC where there is a valid warrant in place in line with the requirements of the FIC Act. The AI, during their process of inspection or review by the FIC may provide the FIC access to the audit trail to provide evidence of verification.

Solution Benefits

Besides the support of the Bill there are specific benefits which the BFS intends to provide. The benefit analysis indicates the positive value that is expected from the BFS and informs the assessment of the BFS and whether it is viable. Furthermore, the benefits can serve as a benchmark to establish at a future point in time whether the benefits were realised. It enables stakeholders to identify what positive outcomes the solution may present.

Figure 3 - Benefit Analysis presents a summary of the BFS benefits identified for the Industry. These are further explored in the next section.

Figure 3 - Benefit Analysis

Detailed Industry Benefits and Associated Measurements

Benefit Description	Metrics
Verification performed using trusted data	• Reduced opportunity to perpetrate fraud using forged documentation • Reduced risk of penalties through evidence of compliance via the audit trail • Increased opportunity to identify the individual attempting to perpetrate fraud
Access to multiple (approved) data providers with coverage of a wide range of data elements	• Reduced risk of money laundering through informed risk decisions • Improved confidence that data is obtained from approved sources • Multiple sources to confirm the same data element
Flexible subscription model	• Adaptability and configuration supports each AI's risk based approach
Enabling "Always Know Your Customer"	• Proactive notification of customer information changes • More dynamic and effective risk management
Overall improved KYC risk management	• Decreased money laundering • Reduced risk of financial crime • Reduced reputational risk
Reduced reliance on paper for evidence of verification for KYC	• Reduced cost of KYC • Reduced cost of remediation • Reduced cost of paper and storage
Single point of integration	• Reduced contract management costs • Reduced system development costs • Reduced infrastructure costs • Reduced support costs
Flexible subscription model	• Reduced time spent negotiating contracts • Pay-for-use model enables cost management
Decreased resourcing requirements	• Reduced KYC resource costs • Reduced KYC training costs
Buy-in and support of FIC and other key regulatory and supervisory bodies	• High number of AIs subscribing to the BFS across the industry • High volume of transactions using BFS • Re-use of verification audit trail data creates economies of scale and efficiency

Conclusion

BankservAfrica in their development of the BFS have followed a robust process which has involved the key industry participants to ensure that the solution that will be developed meets the overall needs of its users and subscribers. Although the BFS is still to be prototyped and developed in a proof of value phase, there is clear evidence that benefits will be derived from the solution.

With the release of the Bill, the design principles that underpin the BFS further assists the AIs in their endeavour to remain compliant. The BFS provides a comprehensive solution that will enable financial inclusion as required by National Policy. The economies of scale and reuse of recently acquired data between AIs enables smaller financial institutions to participate in the market. This will enable further competition and drive down costs for customers and costs associated with switching.

At its core, the BFS supports the requirements of FICA by identifying clients which have a potential risk to engage in money laundering activities and the financing of terrorist activity. By preventing access to information by the general populous, the integrity of the data in the system is maintained. Access to information by investigating authorities will be available at any point in time thereby assisting in investigations and providing feedback to AIs relating to the freezing of funds and property of individuals.

Appendix A – Glossary of Terms

Term	Description	Acronym	Example
Accountable Institution	refers to any of the institutions as listed in Schedule 1 of the Financial Intelligence Centre Act (No 38 of 2001), as amended by the FIC Amendment Act (no 11 of 2008).	AI	Banks, Attorneys, Estate Agents, Stock Brokers
Adverse media service	is when global news sources, current events and relevant media are searched to enable subscribers to perform enhanced due diligence on a customer.		
Association for Savings and Investment South Africa	is a South African industry body representing the majority of the country's asset managers, collective investment scheme management companies, linked investment service providers, multi-managers and life insurance companies.	ASISA	
Audit Trail	is a record of all Solution interactions.		
Banking Association of South Africa	is an industry body representing all banks registered and operating in South Africa.	BASA	
Customer Enquiry Service	is a service available only to the FIC in which they may request information on a specific customer or legal entity and all possible information available at selected data providers will be returned. The information will not be matched or filtered.		
Customer	is the person or entity with which an AI has a business relationship, and/or the entity conducts a single transaction with, that results in a compliance obligation on the AI to identify and verify the said person or entity that is required to ID and V for FIC Act purposes.		AI Customer
Data Provider	is an approved party from whom the Solution shall source data.	DP	
Domestic Prominent Influential Person	means an individual who holds, including in an acting position for a period exceeding six months, or has held at any time in the preceding 12 months, in the Republic— (a) a prominent public function including that of— (i) the President or Deputy President; (ii) a government minister or deputy minister; (iii) the Premier of a province; (iv) a member of the Executive Council of a province; (v) an executive mayor of a municipality elected in terms of the Local Government: Municipal Structures Act, 1998 (Act No. 117 of 1998); (vi) a leader of a political party registered in terms of the Electoral Commission Act, 1996 (Act No. 51 of 1996); (vii) a member of a royal family or senior traditional leader as defined in the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003); (viii) a head or chief financial officer of a national or provincial		

Term	Description	Acronym	Example
	department or government component, as defined in section 1 of the Public Service Act, 1994 (Proclamation No. 103 of 1994); (ix) a municipal manager appointed in terms of section 82(1) of the Local Government: Municipal Structures Act, 1998 (Act No. 111 of 1998); (x) the chairperson of the controlling body, chief executive officer, chief financial officer or chief investment officer of— (aa) a public entity listed in Schedule 2 or 3 to the Public Finance Management Act, 1999 (Act No. 1 of 1999); or (bb) a municipal entity as defined in section 1 of the Local Government: Municipal Systems Act, 2000 (Act No. 32 of 2000); (xi) a constitutional court judge or any other judge as defined in section 1 of the Judges' Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001); (xii) an ambassador or high commissioner or other senior representative of a foreign government based in the Republic; (xiii) an officer of the South African National Defence Force above the rank of major-general; (b) the position of— (i) chairperson of the board of directors; (ii) chairperson of the audit committee; (iii) executive officer; or (iv) chief financial officer, of a company, as defined in the Companies Act, 2008 (Act No. 71 of 2008), if the company provides goods or services to an organ of state and the annual transactional value of the goods or services or both exceeds an amount determined by the Minister by notice in the Gazette; or (c) the position of head, or other executive directly accountable to that head, of an international organisation based in the Republic;		
Financial Intelligence Centre	is a body founded (in terms of Section 2 of the Financial Intelligence Centre Act 38 No38 of 2001) to establish and maintain effective policy, compliance framework and operational capacity to oversee compliance and provide high quality, timely intelligence.	FIC	
Financial Intelligence Centre Act	is an act introduced to establish a Financial Intelligence Centre and a Money Laundering Advisory Council in order to combat money laundering activities and the financing of	FICA, FIC Act	

Term	Description	Acronym	Example
	terrorist and related activities; to impose certain duties on institutions and other persons who might be used for money laundering purposes and the financing of terrorist and related activities; to amend the Prevention of Organised Crime Act, 1998, and the Promotion of Access to Information Act, 2000; and to provide for matters connected therewith.		
Foreign Prominent Public Official	means an individual who holds, or has held at any time in the preceding 12 months, in any foreign country a prominent public function including that of a— (a) Head of State or head of a country or government; (b) member of a foreign royal family; (c) government minister or equivalent senior politician or leader of a political party; (d) senior judicial official; (e) senior executive of a state owned corporation; or (f) high-ranking member of the military;		
Industry Steering Committee	is an advisory committee made up of industry stakeholders and / or experts including representatives from BASA, FIC, ASISA, JSE, BankservAfrica, FSB, BSD and National Treasury. They have an oversight role in the National FICA Solution.		
Johannesburg Stock Exchange	is a securities exchange that offers secure, efficient, primary and secondary Capital markets across a range of securities, supported by post-trade and regulatory services.	JSE	
Know Your Customer	is the due diligence and regulation that AIs and regulated companies must perform in order to identify and verify customers.	KYC	
Manage	is a means to search, create, read, update and delete or cancel, as applicable.		
Match Percentage	is the percentage character overlap between the AI data and the data provided by the data provider.		
BankservAfrica FICA Solution	is this proposed FIC Act Solution which aims to simplify some of the FIC Act process.	Solution, BFS	
Notification Service	is a service in which a subscriber can select specific trigger events and frequencies of customer information changes in order to accommodate risk based approach requirements.		
Politically Exposed Person	is the term used for an individual who is or has in the past been entrusted with prominent public functions in a particular country.	PEP	Members of parliament
Requirement	is something that is wanted, needed or desired.		
Screening service	is the act of checking a customer's information against an AI accepted list.		PEP List, Sanctions List, Interpol List
Service	is a facility offered by the Solution including adverse media services, notifications, screening against screening lists, customer enquiry and/or to perform validation checks against Data Providers.		Adverse Media Services, Notification, Screening and Validation.
Subscriber	is the FIC, any other institution registered with the FIC, or regulatory bodies authorised by the FIC to use the Solution.		NFS Subscriber
Validation Service	is to, upon request, supply information obtained from a		

Term	Description	Acronym	Example
	selected Data Provider (excludes matching of records).		
Verification	is to confirm a customer's information against selected Data Provider information and make a selection of the information that will allow the AI to confirm information they believe to be most accurate.		
Verify	is the process followed to obtain evidence which allows the Subscriber to confirm the identity and other information provided by the customer and which is evidenced, for example, through the provision of copies of documents.		
Watch list	is a list of flagged customers potentially requiring enhanced due diligence to be performed on them.		PEP lists, Screening lists and FIC watch lists