Specification for provisioning of Risk Mitigation Services

Introduction

The payment of the R350 Special Relief Grant to an excess of 10 million clients will be done through multiple channels, such as EFT transfers into established bank accounts; cash transfers into mobile phones and over the counter at various retail outlets. For each payment channel, a number of checks and balances have been put in place to ensure that the grant is paid to the right person.

SASSA already has the ability to directly interface and validate client personal information, such as Name, Surname and Identity number verification against the databases at the Department of Home Affairs.

SASSA also currently verify bank account details of its clients through an account verification service with the banks through the National Treasury Department.

However, payment by money transfer through the contracted banks has been identified as a potential high risk payment option. Various discussions have been held with the banking industry to identify services which could assist in mitigating the risk.

Requirements

SASSA ICT Branch needs to provide assurance to the remainder of SASSA against the risk of fraud in various areas of high risk, which amongst others include confirming that a mobile number belongs to the applicant and that the mobile number provided has not been flagged as suspect in other transactions.

This requirement is not only limited to the payment of money transfer in the SRD R350 environment, but could include any other area of potential high risk which might be identified by SASSA as it includes more risk mitigation services in ensuring that it deals sufficiently and significantly with fraud and risk concerns in the SRD R350 environment, as well as any other environment in SASSA which could include the standard SASSA social grants, staff payments etc. Given that the service might be required for clients / staff in various environments there is no fix amount of verification to be done per month, costing should be provided on a per person basis being verified.

The services required are thus:

1. Verify applications received, where the payment method chosen is through money transfer, against various databases to confirm if the applicant's mobile number and/or email address is legitimate whilst considering originating IP addresses where applicable.

2. Use phone number intelligence, traffic patterns and machine learning to provide a risk profile against a specific cell phone number.

3. Check through various databases available to add additional layers of security which must include validating against the Equipment identity register, thereby providing fraud prevention services which assist with the detection and prevention of application fraud.

4. Provisioning of further fraud prevention services in the format of a model that detects suspicious data and makes predictive fraud risk alerts for instance in line with address and phone frequency.

5. Encompassing the above services, the MRI services as part of the Fraud Prevention Model and the Device Risk Services as previously provided to SASSA should be included in the proposal.

6. The service provider must have the ability to interface with SASSA through batch processes and API's where applicable.

Deliverables

The service provider should provide an all-inclusive proposal for the above solution taking into consideration that the service will be required for a period of 5 years from 1 December 2022 to 30 November 2027.

The service provider should highlight the cost per transaction per SASSA client being verified, as well as provide the response time per verification.

The Service Provider should include its Sole Service Provider Letter in the response to this request for information.

The service provider should lastly complete all required documentation as indicated as required by the SASSA Supply Chain Management Department.

END