

NATIONAL ASSEMBLY

QUESTION FOR WRITTEN REPLY

QUESTION NUMBER 374

DATE OF PUBLICATION: 26 FEBRUARY 2010

Dr D T George (DA) to ask the Minister of Finance:

- (1) Whether the SA Reserve Bank has reported on the system failure that occurred on 3 November 2009; if not, why not; if so, what are the relevant details;
- (2) whether a risk assessment (a) of the system and (b) on the physical location of the system has been conducted by the bank; if not, why not; if so, what are the relevant details?

NW446E

REPLY

- (1) The system failure the Honourable Member is referring to is presumably with regard to the payment system and the software problem at Bankserv (which is the largest of the three central clearing operators, the other two Visa and MasterCard). The Honourable Member is no doubt aware that the SARB functions independently of the executive in terms of its primary objective in terms of section 224 of the Constitution, and does not report to the National Treasury on most functions, unless it is an agency function delegated to it. The SARB does, however, communicate regularly with the National Treasury.

In response to this question, the SARB has indicated that Bankserv and the Payments Association of South Africa (PASA) did report to the SARB the system failure experience at Bankserv on 3 November 2009. Bankserv, the largest of the three central clearing operators, is a company owned by the major banks and not government, monitors its clearing system on a 24 hour basis, and hence became aware of the problem almost immediately. It then notified PASA within 15 minutes, and PASA in turn notified the SARB within 30 minutes of the problem occurring. Within 30 minutes, the banks were requested to switch to an alternate Bankserv site, and this was implemented within 55

minutes of the incident occurring. Whilst most of the problem was resolved, some intermittent problems were experienced at the alternate site. Within 3 hours of the problem, the initial problems at the primary site were stabilised, and banks were requested to switch back to the primary site. Thereafter, total reconciliation of customer accounts was completed by all banks within 5 days.

The incident referred to in this question affected two payment systems, namely debit cards and credit cards. Due to the high volumes and potentially high impact on citizens, these are regarded as systemically important by the SARB despite the fact that the total retail payment environment represents less than 7% of total settlements at the SARB. As a matter of routine, after the problem was resolved, the SARB initiated a review to address weaknesses that were identified during this breakdown, and has taken corrective steps including the need to improve communication with retailers affected by Bankserv.

- (2) In answering this question, the SARB has indicated that the National Payment System (NPS) is not a single system, but consists of 19 different systems (e.g. Real Time Gross Settlement, Electronic funds transfer, Debit and Credit Card, cheques etc). All of the 19 systems in the NPS are constantly monitored, and participation and access regulated according to very strict criteria. Each system has its own set of participants, transactions, legal foundation, rules and technology components. Depending on the values and/or volumes of transactions, some of the systems are designated as systemically important and receive even greater attention from the SARB.

The risk management plan is referred to as the Disaster Recovery Procedures (DRP) and Business Continuity Processes (BCP) plans, and all participants, operators and providers of services are subject in each system to the DRP and BCP, which are also tested at regular intervals to ensure that the processes work in practice.

The SARB has indicated that a risk assessment was therefore in place before the system failure, for the system including its physical location.

Since the incident, the SARB met with the major banks and PASA to ensure that every effort is made to ensure that such incidents do not re-occur. A project has been launched to thoroughly review, implement and test all existing and proposed new

DRP/BCP measures. The intention is to, as far as is humanly possible, exclude any possibility of a similar occurrence in future by mitigating against possible component failures or, in case of failure, have alternative or back-up services immediately available.