GroundUp

Featured On

Interviewed On

Presented In

PARLIAMENT
OF THE REPUBLIC OF SOUTH AFRICA

Social grant fraud: SASSA needs to act, not deny

Instead of wrongly accusing us of illegal hacking, SASSA should take urgent action to fix the extremely serious problems we described

18 October 2024 | By Joel Cedras and Veer Gosai

The South African Social Security Agency has reacted defensively to serious findings about the integrity of its SRD system.

Our article on the failures of the South African Social Security Agency (SASSA) Social Relief of Distress (SRD) grant system has unfortunately been met with a very defensive response from SASSA..

Here's a quick summary of the problems we found:

- First, SASSA's SRD computer system is insecure. It allows anyone to rapidly read massive numbers of records without any authentication.

- Second, there are far more grant applications recorded on the system than is plausible, indicating that a huge number of fraudulent grant applications have been made.
  We provided extensive evidence for this: SASSA's system shows that over 90% of people with IDs indicating they were born in February 2005 have applied for the SRD grant. Also we surveyed 60 people we know: 58 of them had active grant applications for the SRD grant on SASSA's system; 56 stated that they had never actually applied for the grant themselves.
  We also checked the first 500 male and 500 female IDs of people born on 1 January, from 1960 to 2006. On average the SRD application rate was 52% for all of the years, but when looking at people born between 2002 and 2006, the application rate was about 90%. It's simply not possible that this was done legitimately.

- Third, at least some of these fraudulent applications are succeeding, probably very many of them. For example, we discovered that SRD grant payments are being paid for our ID numbers even though we have never received SRD grant payments.
  The scale of the fraud is likely large. Not only is the publicly funded social grant system being looted, but it is likely that many legitimate potential recipients of the SRD grant are not getting paid.

SASSA's response

SASSA has responded to our findings through a press release and interviews given by the executive manager for grant operations at SASSA, Brenton van Vrede.

It is not our intention to embarrass SASSA. The problems we have found are serious and require urgent attention. Responding defensively to us doesn't help anyone.

In a media release SASSA stated that what we had discovered was "not something new" and that they were aware of it. Yet SASSA has never previously publicly disclosed what we showed in our article. As a public institution, it was duty bound to disclose these findings.

SASSA claims that it has blocked two-million applications. Both the media release and Van Vrede have stated that people who have had fraudulent applications made against their ID numbers can contact SASSA and have their identity confirmed through a facial recognition system that it is piloting. No details have been provided on how this works and how widely it has been rolled out.

One of us called the SASSA national hotline three times, and reported the fraudulent application against our ID each time. On a fourth call we were told that, despite the three prior calls, the application was still not marked as fraudulent. Asked about the facial recognition process, the person we spoke to said that they "don't have that system on [their] side".

We cannot overstate our scepticism of the facial recognition process.

Van Vrede also accused us of hacking and committing a crime. This is incorrect. The way in which South African ID numbers are formed is well-documented, and this can be done using a simple algorithm. We wrote a program to do this sequentially, and these were the ID numbers that we then ran through SASSA's system. Nothing was done illegally, and there was no hacking. We are simply ordinary South African citizens, who used public-facing portals to gather our data and to formulate a conclusion.

The problem is that the public-facing portal has no authentication on it. You don't need to log in to use it and there is no limit on the number of queries you can make against it (other than the speed of SASSA's computer system, the network and your computer).

We were able to query the system with 700 generated ID numbers a minute. This isn't illegal; it's the way the system has been designed. It exemplifies incompetent and sloppy software engineering. We are sure Van Vrede means no malice towards us, but it appears that someone involved in SASSA's IT systems must be misleading him.

It is, however, likely that illegal hacking has been used to make fraudulent SRD claims. The scale of the problems seem too large for it to have been done without taking advantage of vulnerabilities in SASSA's IT system.

Every finding we made in our original article remains valid. SASSA needs to take urgent action to improve its SRD IT system and, more importantly, address the massive fraud being perpetuated in relation to the SRD grant, which millions of people depend upon.

Cedras and Gosai are first-year computer science students at the University of Stellenbosch. They have been researching weaknesses in IT systems at major South African institutions.