FINANCIAL EXPRESS, Delhi, 30.8.2018
Page No. 8, Size:(12.78)cms X (15.56)cms.

Unique theft vs Unique ID

UP's ration theft was unique, but it couldn't get past Aadhaar

THE FACT THAT such a large theft of PDS rations should take place across 43 districts in Uttar Pradesh is shocking since most believed that once Aadhaar-based solutions were put in place, this would be a thing of the past. The list of ration shop beneficiaries, after all, had the Aadhaar numbers of each person, so once the fingerprint of someone who came to buy rations was captured on the biometric scanner, UIDAI would have sent a message back saying the biometric matched the given Aadhaar number. What the scamsters did, however, was to take the scamming to another level.

Imagine a ration shop that has 10 customers, C1 to C10, and they have Aadhaar numbers A1 to A10. What the scamsters did was to retain the names of the customer, say C1, but instead of her Aadhaar number A1 in the record, this was replaced by a different Aadhaar number, say, A11. When C11 went to collect the rations, UIDAI was actually being asked to authenticate Aadhaar number A11 and, naturally enough, it was authenticated. When the transaction was completed, the records were switched again and person C1's record now showed the correct Aadhaar number A1. The scam was caught when the authorities found that the same person—in our example, C11—was buying rations many times over and way above the prescribed quota allowed. According to *The Times of India*, 1.9 lakh transactions have been traced so far and they pilfered 2.2 lakh tonnes of wheat and sugar in July; that's over 1,183 kg per person as compared to the 25 kg of wheat/rice and 5 kg of sugar that each family of five is allowed to buy in a month. Whether the civil supplies department was monitoring the authentication requests processed by UIDAI or whether this happened after consumers complained they were not getting their rations is not clear, but it is apparent government departments need to be using Aadhaar transactions to generate regular compliance reports.

Indeed, the government needs to speed up its Aadhaar verification of bank accounts and mobile phone numbers for this very reason. Right now, scamsters or terrorists can create bank accounts or buy mobile phones with fake IDs, but once Aadhaar authentication is mandatory, they can easily be identified. Each time an eKYC is done using Aadhaar, the bank or phone company gets details of the person that include the name, address, age and photograph, so weeding out fakes becomes easier. And now that Aadhaar has introduced facial recognition features, the ability to detect fraudsters has increased even more since, at the time of eKYC, the system will itself match the picture of the person opening a bank account or buying a new SIM with the picture in the Aadhaar database.