The Account Aggregator Ecosystem is Safe & Secure for Customers

The Account Aggregator (AA) framework establishes a consent-based data-sharing mechanism in the financial sector of the country. According to the NBFC-AA Master Directions 2016 published by the Reserve Bank of India and the technical specifications notified by the Reserve Bank Information Technology Pvt Ltd (ReBIT), the ecosystem empowers customers to access, manage, and share their data across various financial institutions. In these data-sharing transactions, account aggregators manage explicit, informed consents for the customer.

We are responding to a [few isolated incidents of fraud](#) involving compromised SIMs that were brought to our attention. Fraudsters exploited these compromised devices to use an AA application to access customer data for targeted phishing attacks. It is important to note that this was not a breach of any Account Aggregator systems but a result of a compromised SIM. We are in touch with the leading cybersecurity experts, government agencies, and regulators for customer protection measures.

We are grateful for the supportive stance from key authorities in India and their recognition of the importance of the AA ecosystem. The authorities have also been apprised of the ongoing efforts of the ecosystem to strengthen customer protection, safeguard customer interests, and deter fraud. We are confident that with their continued support, the ecosystem will continue to grow as a key component of India's critical digital public infrastructure.

Account Aggregators Continue to Remain Safe and Secure

It is critical to note that, under strict security controls prescribed by the Reserve Bank of India (RBI), including **end-to-end encryption**, the customer can share her data with a financial institution of her choice and view it on her personal device. The AAs are **data-blind** consent managers and **cannot store or decrypt** this data on the server side. At the same time, they **cannot** initiate or carry out any financial transactions for the customer or anyone else.

Way Forward

Cybercriminals are always devising new ways to defraud customers, and the cyber threat space is constantly evolving. A well-coordinated and preemptive response from all industry participants is critical in preventing such misuse. This approach is essential not only for mitigating threats but also for creating awareness of the inherent robust security of the ecosystem architecture.

– from DigiSahamati Foundation and the Account Aggregator Steering Committee on 5th August 2024.