Advisory: Access to the customer's contact list on the mobile phone[1]

The fintech industry has seen several instances of customers' contacts from the phone being misused to abuse the customers and their contacts, drawing negative attention from the regulator and the government.

Clause 10.1 for the Digital Lending Guidelines (DLG) categorically says that *'In any case, REs shall also ensure that DLAs desist from accessing mobile phone resources like file and media, contact list, call logs, telephony functions, etc. A one-time access can be taken for camera, microphone, location or any other facility necessary for the purpose of on-boarding/ KYC requirements only, with the explicit consent of the borrower.'*

In the background of the above, we strongly advise the FACE members to ensure as under:

1. Digital Lending Apps(DLAs)[2] do not ask[3] for phone contacts permission, do not access the customer's contact list/call logs and do not transfer/store the customer contact details to their servers or any third parties in any form, digital or physical. This must be ensured for all the versions of DLAs available to customers with necessary technical[4] and operational measures to mitigate against potential misuse.

2. Ensure the above for DLA(s) hosted across all app stores, i.e. Google Play & Apple App Store, and other app stores.

3. Your APIs connected to third parties do not support the consumption or dissemination of such data, and inadvertent access to DLAs is also prevented with measures that no personal identifying information (PII) is present in plain text form at rest or in motion.

4. Make clear and suitable disclosure about access permissions on the app store descriptions, privacy policies, relevant loan documents and during the customer journey at all relevant usage points. This will ensure that customers and other stakeholders have information and assurance that DLA is not accessing the contact list.

5. If the member has unsolicited access to the customer's contact(s) from sources other than the customer's mobile phone/devices, like bank account statements/employer letters etc, the member must equally ensure the privacy/safety of this information against any potential misuse.

---

[1] Approved by the FACE Board through email circulation on 14th Feb 2023
[2] Owned by Loan Service Provider (LSP) or Regulated Entity (RE)
[3] Sometimes, app developers turn off this feature via a feature flag or configuration control. This may create problems, and hence it is recommended that such code is completely removed to prevent accidents
[4] Like force-update of DLA to the latest version

6. If DLA has collected such data in the past, it is the member's responsibility to take all necessary measures to avoid any potential data misuse, including for debt recovery purposes by themselves and their collection partners.

7. Given the criticality of the issue, if a member comes to know that a DLA (of a FACE member or outside) is accessing or misusing the customer's contact list, please report them to teamface@faceofindia.org promptly with evidence for necessary action.