Safe Digital Banking — Fraud Prevention

This section should be a dedicated, prominent page summarising fraud prevention in simple language:

Protect Your Account

- Activate **transaction alerts** via SMS and email for every debit/credit.
- Use **virtual cards** or **masked card numbers** for online purchases where available.
- Regularly review your **account statement** and beneficiary list for any unauthorised additions.
- **Freeze international transactions** on your debit/credit card when not travelling abroad.

Secure Your Devices

- Always use a **screen lock/PIN** on your mobile and laptop.
- Install a reputed **antivirus/anti-malware** solution and keep it updated.
- Do not use **rooted or jailbroken** devices for banking.
- Enable **remote wipe** facility on your mobile device.

Recognise Red Flags

- Unsolicited calls/messages from "bank officials" asking for OTP — **always a fraud**.
- Promises of loan waivers, lottery prizes, cashbacks in exchange for credentials — **never respond**.
- Apps requesting excessive permissions (contacts, call logs, messages) — **do not install**.
- Messages with urgent language like "Your account will be blocked" or "Verify KYC now" — **always a phishing attempt**.

If Fraud Occurs — Escalation Matrix

Step	Action	Contact
1	Immediately call bank's 24×7 helpline to block account/card	Bank's toll-free number
2	Report to National Cyber Crime Helpline	**1930, 1945**
3	File complaint online	**cybercrime.gov.in**
4	Report suspicious SMS/call	**Chakshu – sancharsaathi.gov.in/sfc/**

Step	Action	Contact
5	If bank does not resolve within TAT, escalate to RBI Ombudsman	**cms.rbi.org.in**

Implementation Note for UCBs: Under RBI's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices (2023) and the DPDP Act 2023, all the above content must be reviewed and updated at least **annually**, or whenever a new RBI circular is issued. Bilingual display (English + regional language) is strongly recommended to enhance customer awareness reach.

The bank's **Privacy Policy, Grievance Redressal Policy, and Data Breach Reporting mechanism** should be hyperlinked from all the above pages.