

Digital Security, Mobile Banking & Anti-Fraud Defense

STATUTORY MANDATE & CORE PROTECTION RULE

Never share your mobile banking PIN, passwords, or OTPs with anyone. SLBA

- 1. The Golden Rule of Banking Authentication: No commercial bank employee, customer care agent, or field technician is authorized to ask for your mobile banking PIN, electronic card CVV, or SMS verification code. If someone contacts you claiming an account freeze requires your PIN, immediately terminate the call and notify your nearest branch.
- 2. Securing Mobile Banking Apps & SIM Registrations: Ensure that your mobile SIM card is registered in your legal name matching your National Identity Card. If you experience an unexpected loss of network signal ("SIM Swap"), notify your telecom provider and bank immediately to preempt unauthorized digital wallet takeovers.
- 3. Recognizing Phishing & Social Engineering Schemes: Be vigilant against SMS alerts promising unverified lottery winnings, unsolicited overseas investments, or urgent fee penalties. Authentic bank correspondence will only arrive via verified institutional SMS short-codes and official domain emails ending in accredited bank domains.