FCPED/141/26
April 21, 2026

To: All Banks
Payment Instrument Issuers
Addis Ababa

Subject: Instruction to Financial Institutions on Customer Fraud Awareness Messaging Campaign

Dear Sir/Madam,

While the adoption of digital financial services has grown significantly in Ethiopia, it has also increased consumer protection risks. Recent incidents indicate a rise in scams and attempted fraud conducted through hacked or impersonated messaging and social media accounts. For instance, Fraudsters are increasingly using platforms such as WhatsApp, Telegram, Facebook, email, SMS and unsolicited or fake phone calls to impersonate individuals and request urgent financial transfers from unsuspecting customers. These schemes pose a growing risk to consumers and may undermine public confidence in digital financial services.

As you are aware, the National Bank of Ethiopia (NBE) is mandated to regulate financial education under Article 6(28) of the National Bank of Ethiopia Proclamation No. 1359/2025. In addition, financial institutions are required to inform customers about fraud risks and their responsibilities in safeguarding financial instruments, as stipulated under Articles 5.1.7 and 5.2.8 of Financial Consumer Protection Directive No. FCP/01/2020.

Accordingly, the National Bank of Ethiopia hereby launched Fraud Awareness Campaign and instructs banks and payment instrument issuers to implement the following measures:

1. Customer Fraud Alert Messaging

Banks and Payment Instrument Issuers shall disseminate customer alerts through SMS, mobile application notifications, ATMs and official social media platforms. The alerts shall include clear and actionable messages, including but not limited to the following:

1.1. Customers should not send money based solely on requests received through social media or messaging platforms such as WhatsApp, Telegram, Facebook, email, SMS or unsolicited phone calls. Customers should verify any financial request through direct voice

communication or official contact channels of the purported sender before initiating any transaction.

1.2. Customers must never share PINs, passwords, OTPs, verification codes, or other security credentials with any person under any circumstances.

1.3. Customers should not open suspicious links received through SMS, emails or social media and should only download mobile banking and mobile money applications from trusted sources.

1.4. Customers should regularly check their account or wallet balances and transaction history.

1.5. Customers should not allow strangers or unauthorized individuals to assist them when using ATMs, mobile money and mobile banking applications, or other digital financial services.

1.6. Customers should immediately notify their financial institution if their phone, SIM card, or any device linked to financial services is lost, stolen, or compromised.

1.7. Customers should be encouraged to promptly report any fraud incidents or suspected fraudulent activity related to their accounts to their financial institution through official communication channels.

2. Frequency and Coverage of Alerts

2.1. Banks and Payment Instrument Issuers should disseminate SMS Alerts at least once per month and Social Media Alerts twice per month. The implementation shall follow the phased coverage below:

Channel	Message Type	May–Dec 2026	Jan–Mar 2027	Apr–Jun 2027
SMS or social media (Specify)	Messages outlined under Section 1.1 to 1.7	At least 50% of customers	At least 75% of customers	100% of customers

2.2. Alerts indicated in Section 1.1 will be the first one to be disseminated and to be repeated every other month in the case of SMSs and every month in the case of social media alerts.

2.3. Priority shall be given to high-risk and newly onboard customers where applicable.

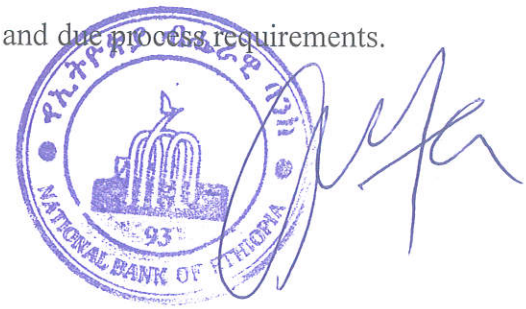
2.4. Banks and Payment Instrument Issuers shall ensure that all alerts are clear, concise, and actionable and disseminated in appropriate local languages.

3. Fraud Mobile Number Identification and Reporting

3.1. Banks and Payment Instrument Issuers are encouraged to identify and take appropriate action on phone numbers and accounts associated with fraudulent activities, including scam messages, fraudulent calls, and impersonation attempts.

3.2. Such cases shall be reported to relevant stakeholders, including Mobile Network Operators, other Banks and Payment Instrument Issuers and law enforcement and security agencies.

3.3. Any action taken shall follow applicable laws and due process requirements.



4. **Reporting Requirements**

4.1. Financial institutions shall submit a report to the National Bank of Ethiopia within Ten (10) days after each monthly SMS alert. The report shall include information about both SMSs alerts and social media alerts in the format attached with this letter.

4.2. Compliance with this instruction shall form part of institutions' consumer protection and fraud risk management obligations. Failure to comply may result in appropriate supervisory or corrective actions by the National Bank of Ethiopia.

Sincerely,

Muhidin Shifa
Director, Financial Consumer Protection and Education Directorate

CC

- **H.E. The Governor**
- **Chief Financial Market and Operations Officer**
  National Bank of Ethiopia

Annex I: Reporting Template for Fraud Awareness Messaging Campaign

Channel	**Message Type**	**Number of Customers Reached**			**Observed Fraud Incidents**	**Customer Responses**	**Trend in Fraud Incidents**
		Male	Female	Total			
SMS							
Social media							
Others (Specify)							

A) Report Prepared By
Name:.....Position:.....
Date:.....Signature:.....Mobile/phone:.....

B) Report Approved By:
Name:.....Position:.....
Date:.....Signature:.....Mobile/phone:.....