This document has been translated for knowledge, for legal purposes the Arabic version prevails

Number: 10/6/ 14206
Date: 27/1/1445 H
Corresponding to: 14/8/2023 AD

# Circular to:
# Banks operating in the Kingdom
# Mobile payment services companies
# Subject: Account activation mechanism on electronic channels

**After greetings,**

Within the framework of the Central Bank's effort to regulate and develop the national payments system; to ensure the provision of safe and efficient systems, services and channels for payment and transfer in the Kingdom, and in view of the increasing use of electronic channels by customers in various fields, I would like to stress the need for you to implement the following procedures and controls as a minimum, as follows:

**First:** When the customer creates an account on one of the electronic channels (for example, but not limited to: mobile phone application, online banking,...) or reactivates his account on it, or in the event of recovering/changing the user name or recovering the password for the customer through these channels, or when accessing it from a device other than the one stored in your records, you must verify the customer's identity by activating the following controls:

1) Request at least three pieces of information from the following categories of data, including at least one piece of information from each category and matching it with the data you have registered:
    a. The customer's personal data, including but not limited to (National number/passport number for non-Jordanians, date of birth, document number, document expiration date)
    b. Data related to the account, including but not limited to (bank account number, international bank account number (IBAN), customer password (PIN Code)).

c. Banks are obligated to request data related to payment cards, for example, but not limited to (payment card number, CVV number mandatory followed by the customer's secret number (PIN code)), and mobile payment service companies have the option to apply this clause if cards linked to the electronic wallet are available.

2) After verifying and matching the data specified in Clause (First/1) above, a one-time password (OTP) should be sent to the customer on his phone number identified according to your records. If the customer's biometrics are available, you can request the biometrics from the customer without the need to send a one-time password (OTP).

**Second**: When a customer changes the phone number registered in your records through his use of one of the electronic channels and for the purposes of verifying the customer's identity, this requires first following the procedures stipulated in Clause (First/1) above and then sending a one-time password (OTP) to the new number in addition to sending an SMS to his old number to inform him of the process of changing his phone number known to you, as well as sending an e-mail to the customer according to the e-mail identified in your records - if any, to inform him of the change process.

**Third**: If the customer is allowed to access his account on more than one device, a one-time password (OTP) must be sent when entering the account from a device not known to you, and an SMS message must be sent to inform the customer of the attempt to enter the account from another device, in addition to the necessity of setting a maximum limit on the number of devices authorized to access the account so that it does not exceed three devices, and does not allow simultaneous access, as well as enabling the customer to manage the authorized devices to access his account.

**Fourth:** Monitoring the effectiveness of customers' phone numbers linked to their accounts and periodically verify the effectiveness of using electronic channels through the same number known to you, by requiring all customers to enter a one-time password (OTP) for a maximum of (90) days when accessing their accounts on electronic channels, provided that a grace period is set after (90) days, up to (30) days, during which a one-time password (OTP)

will be sent upon any attempt by customers to access their accounts before the account status becomes “Inactive”. Customers will then need to reactivate the accounts via the controls referred to in Clause (First) above to reactivate the accounts.

**Fifth:** Periodically review customers’ access to their accounts on electronic channels and document the review results, in order to ensure that electronic channels are not used by anyone other than your customers and to detect any unusual usage attempts based on the customer’s behavior and activity, including but not limited to (reports of repeated incorrect customer login operations to their accounts, reports on the use of electronic channels from multiple geographical locations, reports on the frequency of modifying phone numbers over relatively short periods of time, etc.) and take the necessary measures by you.

**Sixth:** Your commitment to adjusting your position in accordance with the provisions of this circular within a period not exceeding (6) months from the date of its issuance.

**Respectfully,,**

**Governor**
**Dr. Adel Al Sharkas**