SmartMessage

# Effective Prevention of SIM SWAP Frauds for the Largest Private Bank of Turkey through SmartMessage's Reliable Solution

TÜRKİYE İŞ BANKASI

As a financial institution with a deep-rooted history, İşbank has one of the **highest number of domestic branches** (1249)* and ATMs (6506)* in Turkey servicing over **20 million customers*** out of which **8,1 million are digital-only customers***. This number reflects the company's achievements in adopting new technologies and pioneering digital transformation in the turkish banking industry.

SmartMessage Secure's effect was so impactful that Isbank decided to deploy more than one licensing for different departments' use.

* Source: İşbank 2019 Investor Presentation

**Solutions**

SmartMessage Secure

**Results**

Massive improvement in SIM card-related fraudulence prevention. (Rate dropped to **0,1%)**

SmartMessage Secure prevents **160-170 frauds per day** maximizing the operator change security.

SmartMessage Secure provides flawless **high volume OTP delivery performance** that fulfills Isbank's needs.

For more information feel free to visit https://www.smartmessage.com/



## SIM-Swap Fraud: What, Who and How?

Faking SIM-swap is a fraud action in which someone contacts your carrier and presents himself as the owner of your mobile number by using your personal data and allowing all messages and calls to be directed to the new SIM card.

## Key Actors to Prevent SIM-Swap Fraud

Mobile Carriers – store GSM data and can share with the Banks during transactions.

Banks - the main authority for transactions, holding sensitive information and customer financials can prevent fraud during OTP authentication.

## Indicators of Potential SIM Fraud

Total loss of signal in mobile phone

Unable to send and receive a call or a message

Identity theft

Loss of online presence

Suspicious withdrawals or bank account depletion

## How SmartMessage solved Isbank's problem

Integrated with the bank's systems, SmartMessage Secure started regular checks for operator and SIM card changes.

With use of techniques like blacklist management and safe transition models like OTP, the fraud rate dropped almost to zero.