

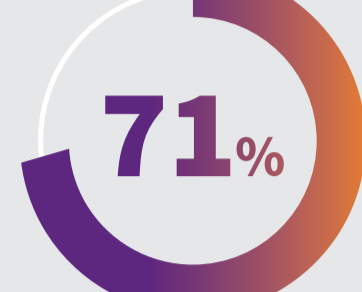
The True Cost Of

# Fraud In Saudi Arabia

In this study, Forrester conducted a global online survey of **1,845** senior decision-makers at financial institutions and retail/e-commerce institutions to evaluate the cost, current state, and challenges presented by fraud. Survey participants from Europe, the Middle East, and Africa (EMEA) include **541** senior decision-makers across **9** EMEA markets.

Below are some of the key results for Saudi Arabia.

As adoption of digital services increases in Europe, the Middle East, and Africa (EMEA) and daily life grows more digitized, cybercriminals see more opportunities to exploit both consumers and businesses. Across the region, more than half of respondents surveyed reported an increase in fraud (by 6% or more) over the last 12 months, **with 52% of fraud originating from digital channels**. However, even as organizations increase their investments in fraud prevention solutions, criminals continually introduce new, more sophisticated fraud methods (e.g., synthetic identities) to circumvent these solutions.



The impact this has on organizations is multifold. Accounting for fines, fees, and effort spent on investigating fraudulent transactions, organizations incur fraud costs between three and five times the actual value lost to fraudsters. This does not even consider the impact on the customer experience, **with 71% of respondents noting a detrimental impact on customer conversion rates**.

## The True Cost Of Fraud In Saudi Arabia

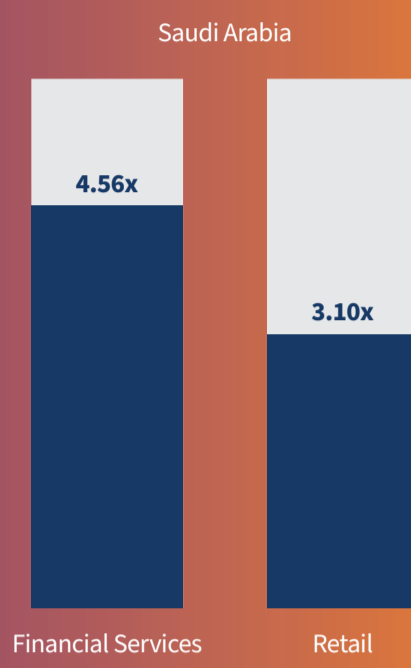
Every fraudulent transaction costs

# 3.83x

the lost transaction value on average.

For retailers, this includes the costs of fees and interest paid as well as cost of replacing lost/stolen merchandise.

With more extensive regulations requiring additional investigative efforts, higher labor costs, and liability in refunding consumers, the total cost of fraud is even higher for financial institutions.



Base: 541 decision-makers across EMEA with responsibility for fraud strategy in their organizations Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis - Risk Solutions, July 2023

## Main Increasing Types Of Online Fraud

### Financial Services

- Overall Fraud Level
- Identity Theft Fraud
- Card Not Present
- Account Takeover
- Mobile Transactions Fraud

### Retail

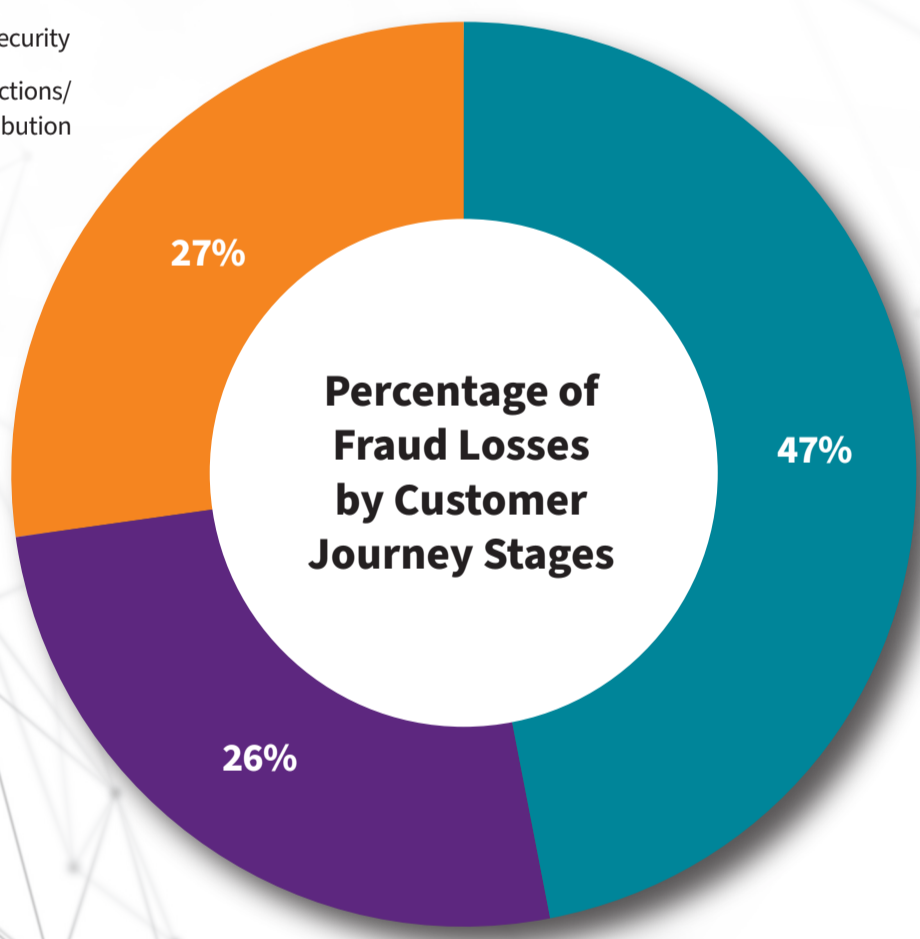
- Fake Reviews and Ratings
- Collusion Fraud
- Promotion Fraud/ Policy-Abuse Fraud

## Stolen And Synthetic Identities Are The Largest Contributors To Fraud Losses

Criminals are capitalizing on the popularity of digital banking and digital commerce to use stolen or synthetic identities to open new accounts.

Nearly half of all losses can be traced back to fraudulent new-account creation.

- New Account Creation
- Account Login/Security
- Purchase Transactions/ Deposit or Distribution of Funds



## Keeping Up With Constantly Evolving Trends And Threats

### Top Fraud Prevention Challenges

- Inability to Stay Current and Defend Against New, More Sophisticated Payment Frauds
- Balancing Fraud Prevention Friction with Customer Experience
- Lack of Specialized Fraud Prevention Tools for International Orders/Transactions
- Privacy Concerns
- Inability to Manage and Prevent Fraud for New Transaction Methods

## Fragmented Use Of Identity And Transaction Verification Solutions

| New Account Creation          | Account Login   | Purchase Transactions & Distribution Funds |
|-------------------------------|---|--|
| Geolocation                   | Geolocation   | Government-Issued Identification Document  |
| Email Risk and Verification   | Device ID/Device Fingerprinting                                   | Name/Address/DOB                           |
| Automated Transaction Scoring | Authentication of Transaction /Customer (Using OTP or Two Factor) | Email and Risk Verification                |

Download **LexisNexis® True Cost of Fraud™ Study** to learn more about how to balance fraud prevention friction and seamless customer experience.

[Download The Study](#)

