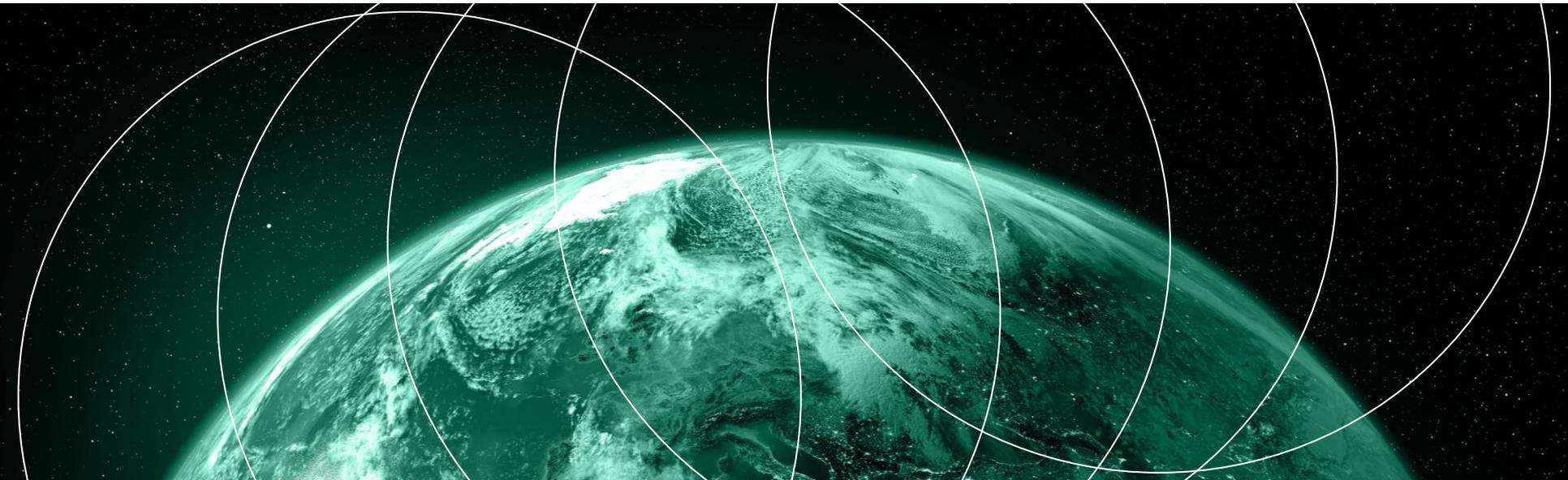


LexisNexis® True Cost of Fraud™ Study Europe, Middle East, And Africa

A COMMISSIONED STUDY CONDUCTED BY FORRESTER CONSULTING ON BEHALF OF LEXISNEXIS® RISK SOLUTIONS, FEBRUARY 2024



Executive Summary

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.

To successfully balance fraud prevention friction against a seamless customer experience, organizations need to implement multifaceted solutions that address different types of fraud risks: physical identity, digital identity, and transactions. Advanced real-time transaction verification solutions utilizing AI and ML are especially crucial as they work in the background to help prevent fraudulent transactions with minimal impact on customers. At the same time, they bring organizations into compliance with new payment regulations like 3DS2 and PDS3.

Commissioned by LexisNexis® Risk Solutions, Forrester Consulting conducted a global survey of decision-makers in fraud strategy. This report highlights findings for EMEA. Detailed demographics are available at the end of the study.

Double-Edged Sword Of Digitalization

As adoption of digital services increases in EMEA, cybercriminals are seeing more opportunities to exploit both consumers and businesses.

Across the region, digital channels (online/mobile) now account for 52% of overall fraud losses, surpassing physical fraud for the first time.



DIGITAL CHANNELS



32%
Online



20%
Mobile

NON-DIGITAL CHANNELS



25%
Physical/in-store



21%
Telephone/
contact center



4%
Other

Fraud Continues To Increase

In our survey of 541 fraud management executives at financial and retail organizations across EMEA, 52% of respondents at financial institutions and 53% of respondents at retailers reported an increase in overall fraud levels in the past 12 months.

Despite higher consumer awareness about data privacy, identity theft persists in the region, with 53% of respondents reporting an increase. Retailers reported seeing the highest increase in card-testing fraud, in which fraudsters attempt to test the validity of stolen or compromised credit or debit card information.

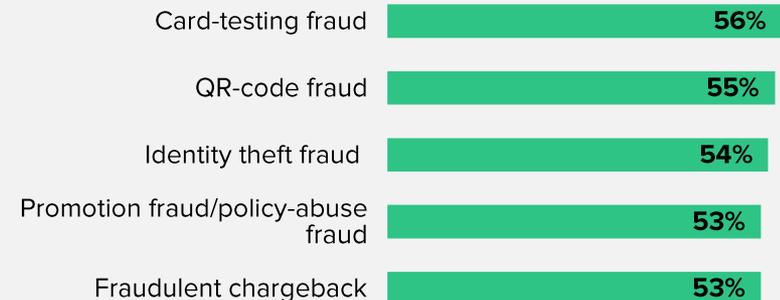
Top Five Fastest-Growing Types Of Fraud In The Past 12 Months

(Percentage indicating organizations who reported a 6% or more increase in fraud type)

FINANCIAL SERVICES



RETAIL



Stolen And Synthetic Identities Are The Largest Contributors To Fraud

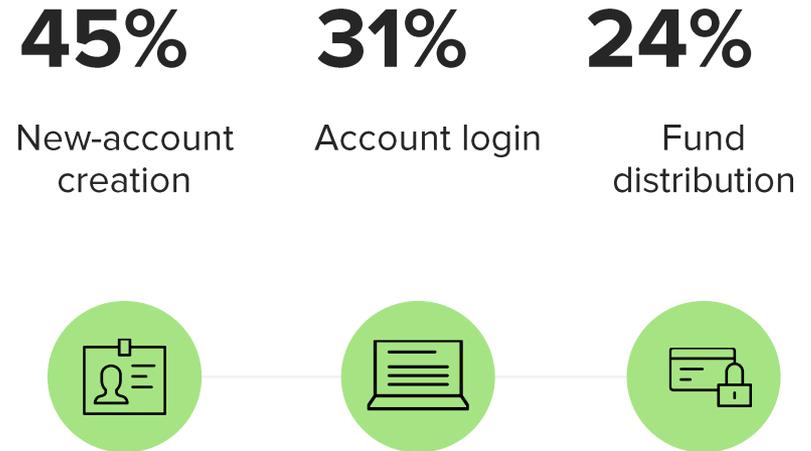
Criminals are capitalizing on the popularity of digital banking and digital commerce to use stolen or synthetic identities to open new accounts.

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

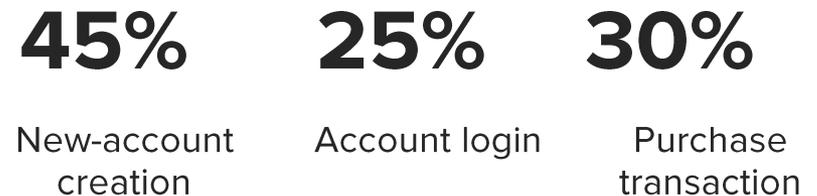
For retailers in EMEA, purchase transactions are the second-most types prone to fraud, whereas for financial institutions, account logins are the second-most vulnerable stage.

Fraud Losses Attributed To Each Stage Of The Customer Journey

FINANCIAL SERVICES



RETAIL



True Cost Of Fraud Goes Far Beyond Face Value Lost

Every fraudulent transaction costs

3.90x

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.

FINANCIAL SERVICES

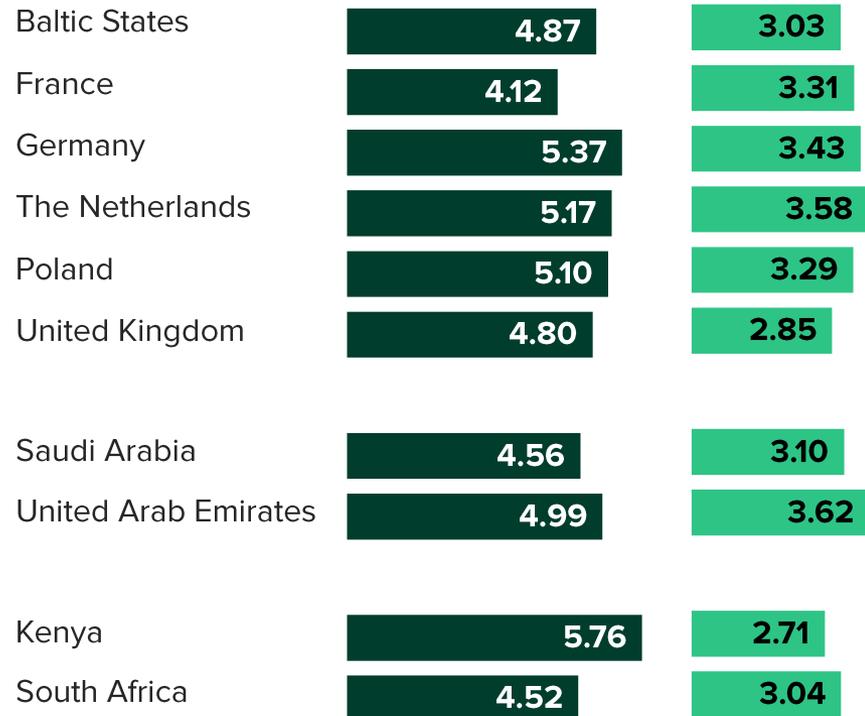
4.92x

the lost transaction value

RETAIL

3.20x

the lost transaction value



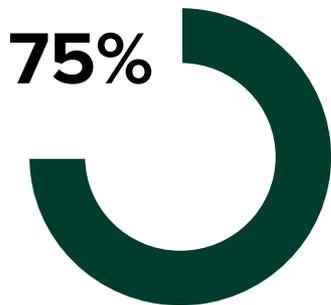
Customer Relationships Are On The Line



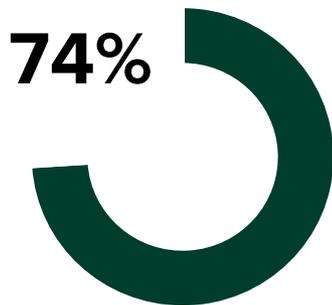
Aside from fees and labor costs, there are indirect, long-term consequences of fraud. Three-quarters of respondents reported that fraud has negatively impacted their brand and customer experience, which impacts revenue down the line.

The Impact Of Fraud On Customer Relationships

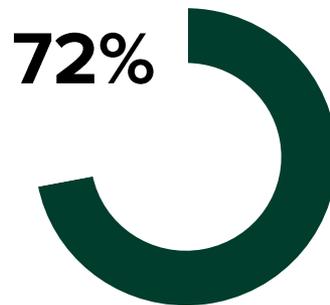
(Showing “Significant impact” and “Moderate impact”)



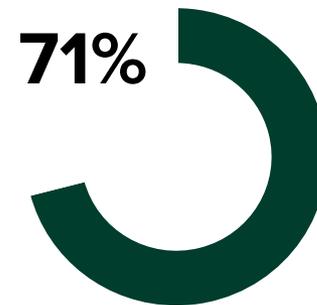
Reduced customer satisfaction due to poor customer experience



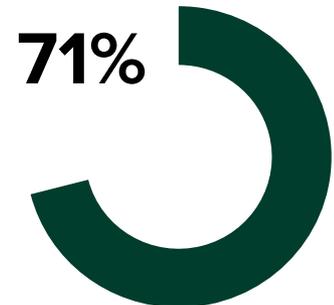
Customer churn



Difficulty establishing trust with customers



Damage to brand/reputation



Reduced customer conversion rate

Organizations Struggle With Constantly Evolving Trends And Threats

Respondents at both retailers and financial institutions called out new, evolving trends (in payment methods and fraud) as a challenge in fraud prevention.

Furthermore, given the stringent privacy regulations in Europe, retail respondents identified privacy concerns (during identity verification) as a top challenge, whereas those at financial institutions struggle with getting the right mix of tools to defend against cross-border fraud.

Main Challenges In Fraud Prevention Over the Past 12 Months

FINANCIAL SERVICES

Implementing the right fraud prevention processes for international transactions



Balancing fraud prevention friction with customer experience



Staying current and defending against new, more sophisticated payment frauds



RETAIL



Consumer privacy concerns (e.g., around data collection, use and sharing, etc.)



Managing fraud for new transaction methods



Technology implementation complexity

Retailers Are Caught Between Customer Safety And Customer Experience

To stave off bot attacks, retailers need to introduce identity authentication across all stages of the customer journey. Yet many verification processes introduce friction to the customer experience, which leads to transaction drop-offs or cart abandonment by legitimate customers.

Top Challenges Along The Customer Journey



Distinguishing between human and bot transactions

Verification of customer identity

Implementing the right fraud prevention processes for international transactions

End-user identity authentication

Distinguishing between human and bot transactions

Balancing fraud prevention friction with the customer experience

Balancing fraud prevention friction with the customer experience

Distinguishing between human and bot transactions

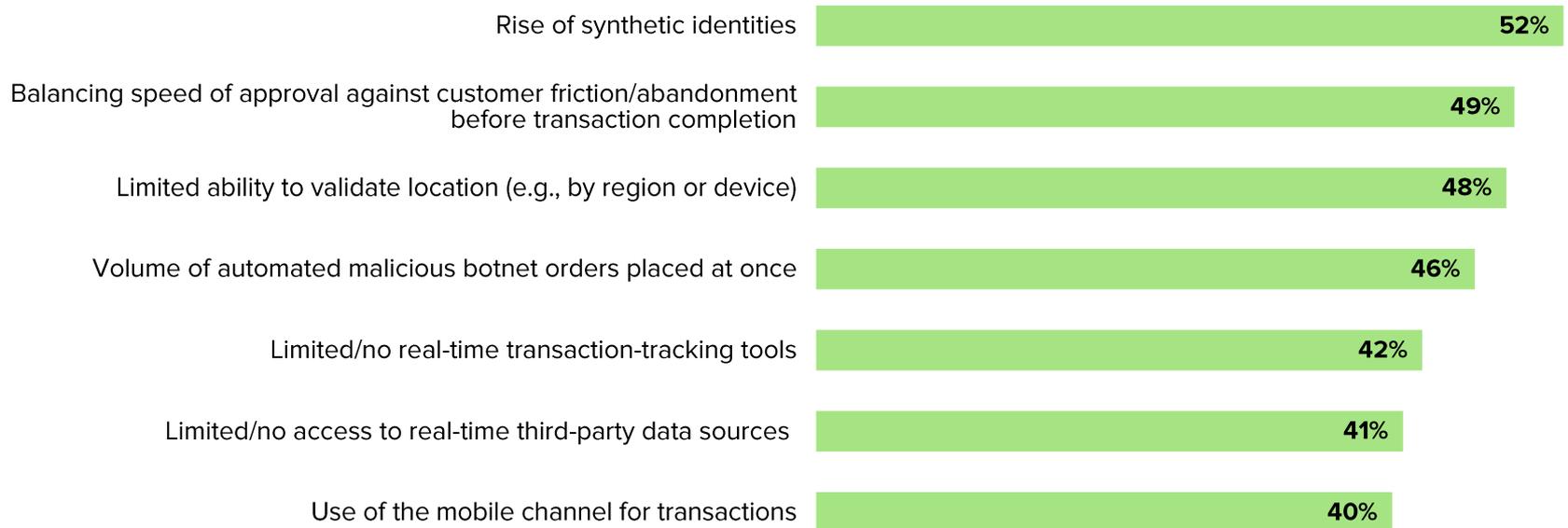
End-user identity authentication

Rise Of Synthetic Identities Impedes Customer Identity Verification

More than half of executives cite synthetic identities as a top challenge in the customer identity verification process. Even with solutions in place to combat synthetic identities, 49% of respondents are concerned with the friction they introduce in the customer journey.

Customer Identity Verification Challenges Through The Online Channel

(Percentage showing ranks 1 through 3)

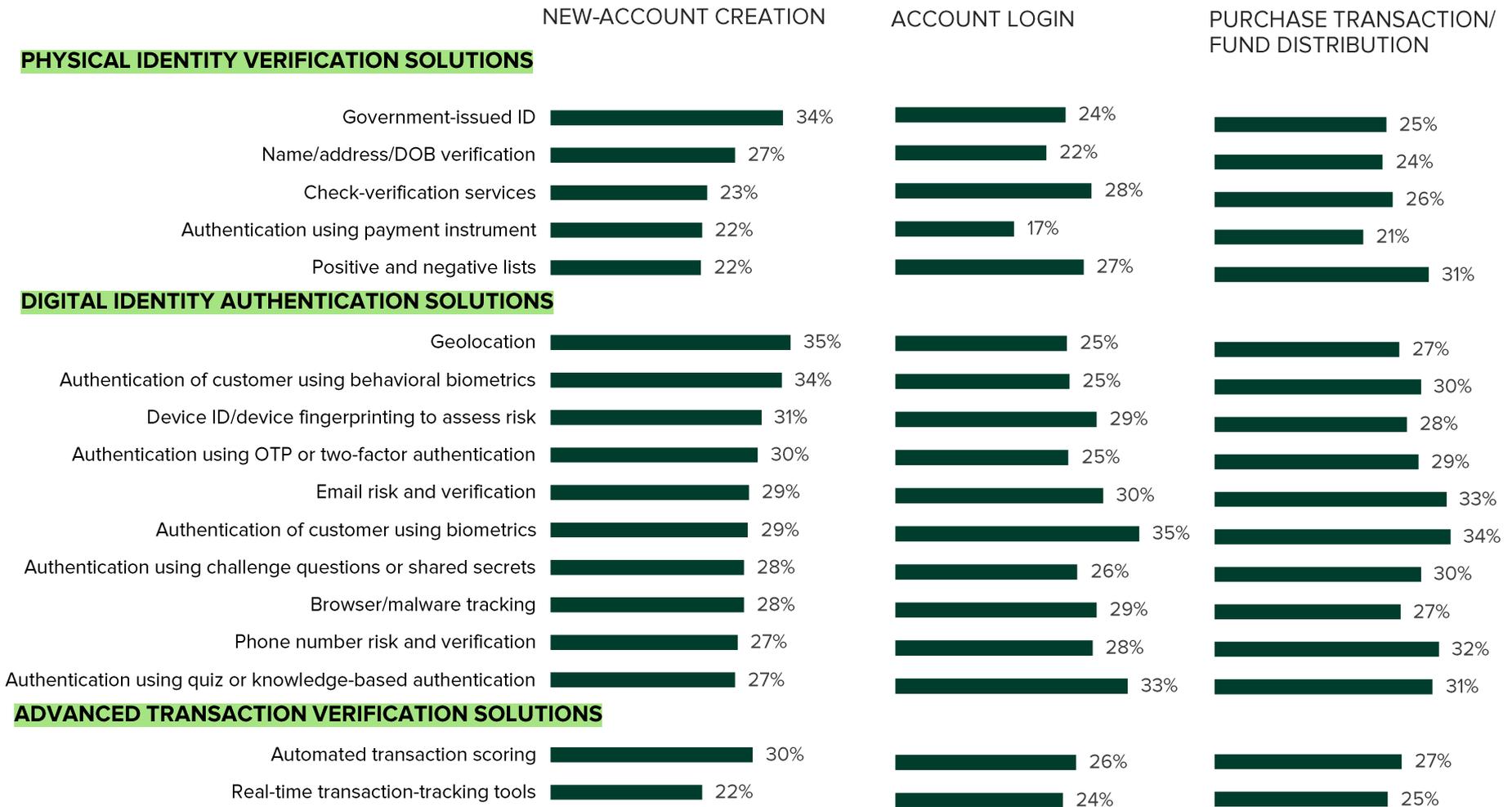


Complexity Of Fraud Calls For Multifaceted Solutions Along The Entire Customer Journey

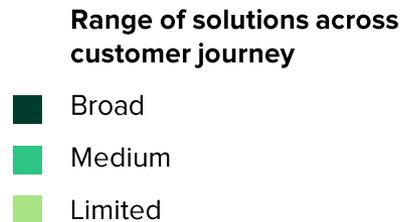
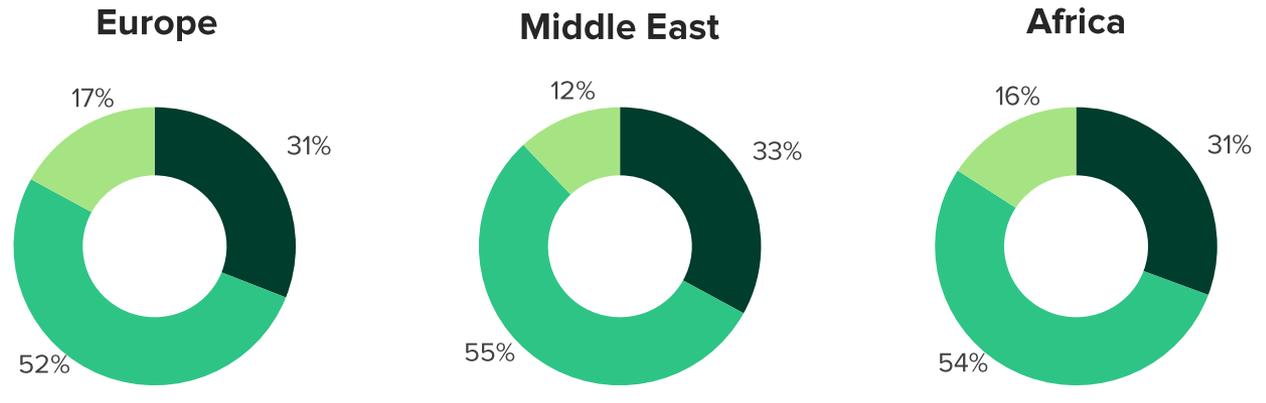
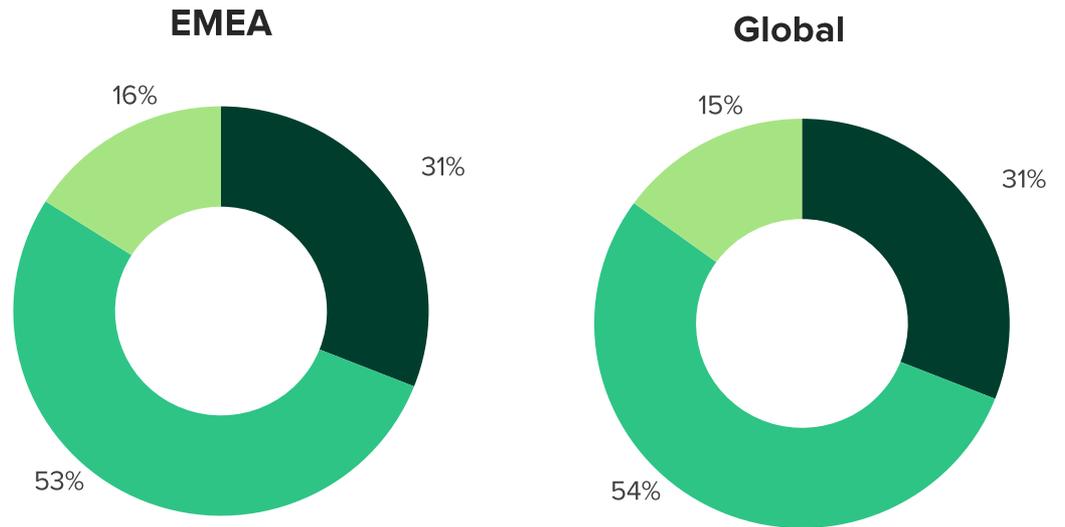
As fraud can take many forms and is continually evolving, organizations need a comprehensive approach to fraud detection and prevention. Organizations will need to adopt a multifaceted approach and implement various solutions to effectively address physical identity, digital identity, and transaction fraud risks.



Adoption Of Fraud Mitigation Solutions Across The Customer Journey



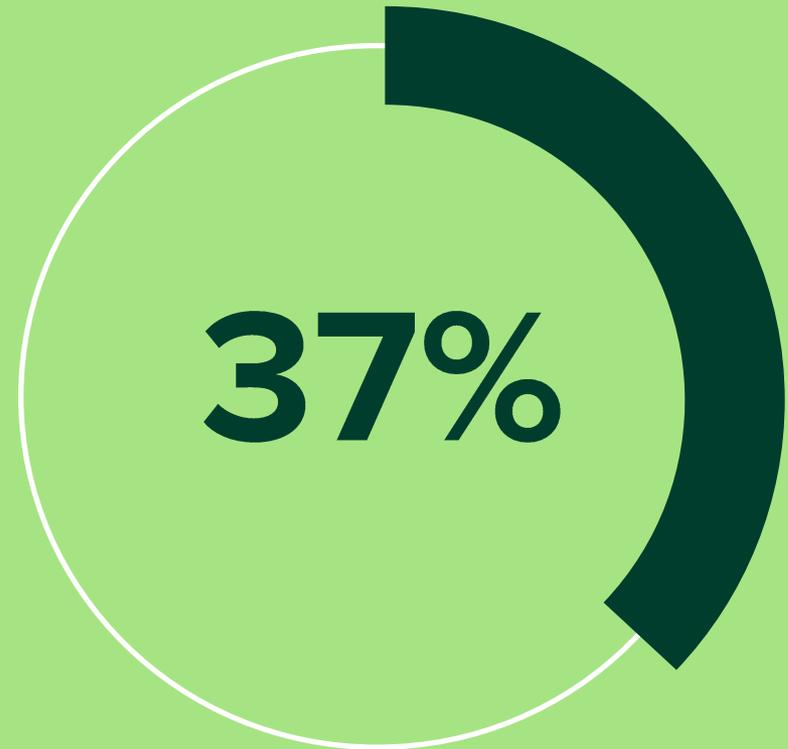
However, across the region, only one-third of organizations have a broad suite of solutions that mitigate against all three different fraud risks across the entire customer journey.





Gaps In Fraud Coverage Leave Businesses Vulnerable

Close to 40% of respondents said their organizations do not have an enterprise fraud management solution that provides a comprehensive coverage of all channels on which customers can initiate transactions.



Adoption Of Digital Technology To Prevent Fraud Is Still Fragmented

Proactively scoring activities and transactions can eliminate unnecessary verification processes for legitimate customers, helping to minimize customer friction and reduce the cost of managing fraud.



Delivery verification **39%**

32% Location analysis

Threat detection **32%**

31% Behavioral biometrics

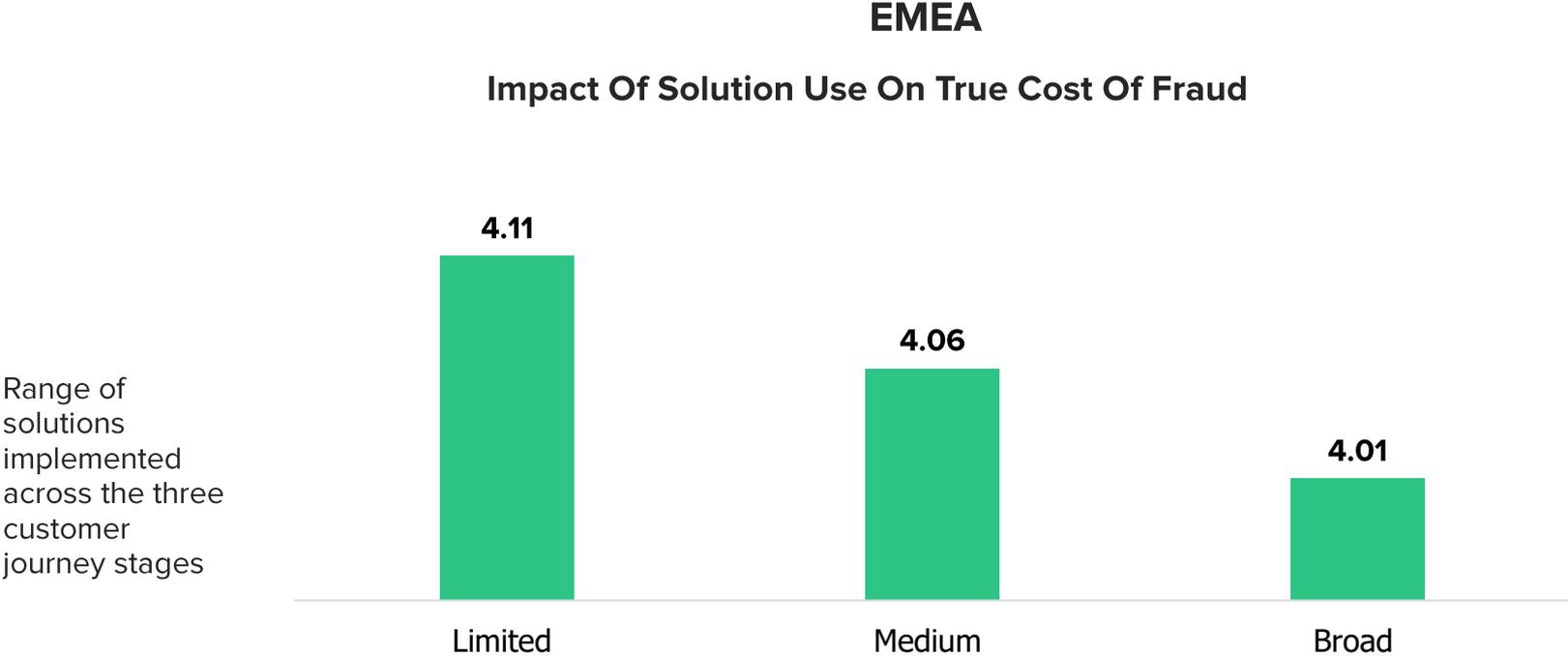
Anomalous activity/transactions **28%**

27% Consortia or exchange data

Proprietary scores **25%**

Implementing A Broad Range Of Solutions Is More Effective At Preventing Fraud

Smart investments in varied solutions pay off: organizations that build a broad net of defense against fraud throughout all stages of the customer journey report a lower true cost of fraud. One reason could be that having the proper fraud management solutions in place may also help increase compliance and limit liability in cases of fraud.



Key Recommendations

Combine a risk-based and data-driven approach to fraud management. Utilize advanced data analytics tools and techniques to identify patterns and anomalies in customer behavior. Apply different levels of security measures based on the level of risk associated with each transaction or customer to minimize the impact on low-risk transactions and genuine customers.

Balance fraud management effectiveness and CX with customer education. Raise customer awareness about emerging threats — especially in areas like scams, mobile transaction fraud, and QR code fraud — and the potential impact they have on their own security to help them understand the necessity of security measures. This is especially crucial as the region moves toward higher authentication requirements with PSD3.

Key Recommendations

Leverage emerging technologies. Traditional rules-based models are costly to maintain and ineffective against new types of fraud. Embrace emerging AI technology, including supervised learning, unsupervised learning, deep learning, and graph computing for more efficient fraud management. Privacy-preserving technologies like homomorphic encryption and federated learning can also bring richer data insights to fraud analysis by breaking down data silos across divisions and organizations and enabling efficient data sharing. New technologies like behavioral biometric authentication can help to prevent more advanced impersonation scams.

Regularly update security protocols and prevention tools/services. Establish governance to regularly update and refine security protocols and prevention tools/services to effectively mitigate the evolving threat landscape, maintain compliance, and enhance overall security posture. Regular updates and refinements ensure that organizations remain compliant and avoid potential legal and financial repercussions.

Methodology

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 across EMEA made up 541 of these respondents. Questions provided to the participants asked about their organizations' priorities, exposure to fraud activities, fraud prevention practices and factors driving an increase in fraud costs, challenges related to fraud operations, the benefits of fraud operations, and future implementation plans. Respondents were offered a small incentive as a thank-you for time spent on the survey.

The study began in July 2023 and was completed in August 2023.

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. LexisNexis is a registered trademark of RELX Inc. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. All other trademarks are the property of their respective companies. [E-57210]

Project Team

[Josephine Phua](#), Market Impact Consultant
Emilie Beaud, Associate Market Impact Consultant

Contributing Research

Forrester's [Security & Risk](#) Research Group

Demographics

| COUNTRY | |
|----------------------|-----|
| Estonia | 3% |
| France | 10% |
| Germany | 10% |
| Kenya | 10% |
| Latvia | 4% |
| Lithuania | 4% |
| Poland | 10% |
| Saudi Arabia | 10% |
| South Africa | 10% |
| The Netherlands | 10% |
| United Arab Emirates | 10% |
| United Kingdom | 10% |

| INDUSTRY | |
|--------------------|-----|
| Retail | 30% |
| E-commerce | 29% |
| Lending | 18% |
| Financial services | 22% |

| COMPANY SIZE | |
|------------------------------------|-----|
| Small: <US\$10M annual revenue | 41% |
| Mid/large: >US\$10M annual revenue | 59% |

| NUMBER OF EMPLOYEES | |
|---------------------------|-----|
| 2 to 99 employees | 0% |
| 100 to 499 employees | 22% |
| 500 to 999 employees | 30% |
| 1,000 to 4,999 employees | 25% |
| 5,000 to 19,999 employees | 14% |
| 20,000 employees or more | 9% |

| RESPONDENT LEVEL | |
|-------------------|-----|
| C-level executive | 23% |
| Vice president | 33% |
| Director | 43% |

Note: Percentages may not total 100 due to rounding