LexisNexis®
RISK SOLUTIONS

2023 LexisNexis® True Cost of Fraud™ Study: Ecommerce and Retail Report

U.S. and Canada Edition

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

The LexisNexis® Risk Solutions True Cost of Fraud™ study included an extensive survey of 358 risk and fraud executives in retail and ecommerce* companies in the U.S. (289) and Canada (69)

RETAILERS AND ECOMMERCE MERCHANTS INCLUDE A VARIETY OF CATEGORIES:	
# of Survey Completions	🏈 📺 🎨 👕 🍾 ⬇ 🍕 ✈ ♫ 💻 🚗 🌷 📱 🎁 🖨 🛠 💡 📞
358	

SEGMENTS		
Segment Definitions	🛒 **Small** Earns less than $10 million in annual revenues	🛒 **Mid/Large** Earns $10 million+ in annual revenues
# of Survey Completions	**179**	**179**

*Retailers can also have revenue from ecommerce channels. For this study, organizations with <60% revenue from digital channels are classified as retailers, while those with >60% are classified as ecommerce merchants.

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

The study helps companies grow their business more safely by navigating the growing risk of fraud

The research provides a snapshot of:

- Current fraud trends in the U.S. and Canadian ecommerce and retail markets
- Key pain points related to adding new payment mechanisms, transacting through online and mobile channels and expanding internationally

Data Collection:

- Data collection occurred between July and August 2023 as part of a larger commissioned global study conducted by Forrester® Consulting
- Many of the survey questions reference the past 12 months

Fraud definitions:

- Fraudulent transactions due to identity fraud, which is the misuse of stolen payments methods (such as credit cards) or personal information
- Fraudulent requests for refunds/returns, bounced checks
- Lost or stolen merchandise, as well as redistribution costs associated with redelivering purchased items
- Fraudulent applications (e.g., purposely providing incorrect information about oneself, such as income, employment, etc.)
- Account takeover by unauthorized persons
- Use of accounts for money laundering

This research covers consumer-facing fraud methods:

- It does **not** include insider fraud or employee fraud

The LexisNexis Fraud Multiplier™ cost:

- The financial impact of fraud is more than the actual dollar value of a fraudulent transaction. It also includes additional costs related to replacing merchandise, fees and interest. Therefore, the total cost of fraud is expressed by saying that for every $1 of lost value due to fraud, the actual cost is higher based on a multiplier representing these additional costs.
- For a common base of comparison between the U.S. and Canada, all currency is in USD

Overview

Key Findings

Digitalization Trends

Attacks and Impacts

Merchant Losses

Challenges Mitigating Fraud

Current Approaches

Recommendations

The True Cost of Fraud™ study defines the customer journey as follows:

New Account Opening

Establishing a new account

Verifying new identity, credentials

Purchase Transaction

Making a purchase

Verifying identity before finalizing the sale

Account Login

Accessing an account

Verifying identity before allowing access

Summary of Key Findings

Digitalization continues to transform the industry. One-fifth of transaction volume occurred via digital payments methods such as digital wallets, payment apps, Buy Now Pay Later (BNPL) schemes and cryptocurrency. Digital transactions drive over half of revenue.

As adoption of digital services increases in North America and daily life grows more digitized, cybercriminals are seeing 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.

The impact of fraud on merchants is multifold: Accounting for fines, fees, the face value of fraudulent transactions, and the costs and effort of replacing lost/stolen merchandise. Organizations are incurring fraud costs of 3x the actual value lost to fraudsters. This does not even consider the potential long-term cost that stricter verification checks have on the customer experience, with 75% of respondents noting an impact on customer conversion rates.

Retailers are caught between customer safety and customer experience while working to fight new fraud methods and integrate new fraud mitigation capabilities. Consumer adoption of a broadening spectrum of payment methods drives merchants to accept novel payments methods, increasing merchants’ attack surface and fraud risk.

To successfully balance fraud prevention friction against a seamless customer experience, forward-thinking merchants are orchestrating multi-faceted solutions via fraud platforms. To help manage risk across different use cases they leverage three complementary lenses: physical identity, digital identity and past transaction behavior. Advanced real-time transaction verification solutions using artificial intelligence (AI) and machine learning (ML) are especially crucial as they work in the background to help prevent fraudulent transactions with minimal impact on customers. Additionally, retailers and merchants can leverage Strong Customer Authentication (SCA) strategies to shift their fraud loss reimbursements liability.

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

Key Recommendations

Combine a risk-based and data-driven approach to fraud management. To better identify patterns and anomalies in customer behavior, use advanced data analytics tools and techniques. Calibrate and apply anti-fraud measures based on the level of risk associated with each transaction or customer to minimize impact on low-risk transactions and legitimate customers.

Balance fraud management effectiveness and customer experience. As digital interactions and transactions become increasingly common, businesses are competing intensively to win and retain new customers; therefore, customer onboarding and payment journeys should be as seamless as possible. However, some fraud management solutions introduce additional verification or authentication steps for customers which can lead to cart abandonment and customer churn. Retailers need to strike a balance between fraud management effectiveness and customer experience. Leveraging solutions that perform without active consumer engagement, such as behavioral biometric-based risk assessments, can help to achieve this goal.

Work with vendors leveraging emerging technologies. AI/ML-based technologies including supervised learning, unsupervised learning, deep learning and graph computing have become the norm in fraud management. Richer data insights into fraud analysis can break down data silos across divisions and organizations and enable more efficient data sharing. New technologies like behavioral biometric risk assessment help to prevent more advanced fraud schemes, and detect scams at the target-coaching stage.

Key Finding 1

Digitalization continues to transform the industry, driving changes in consumer buying and payment behavior.

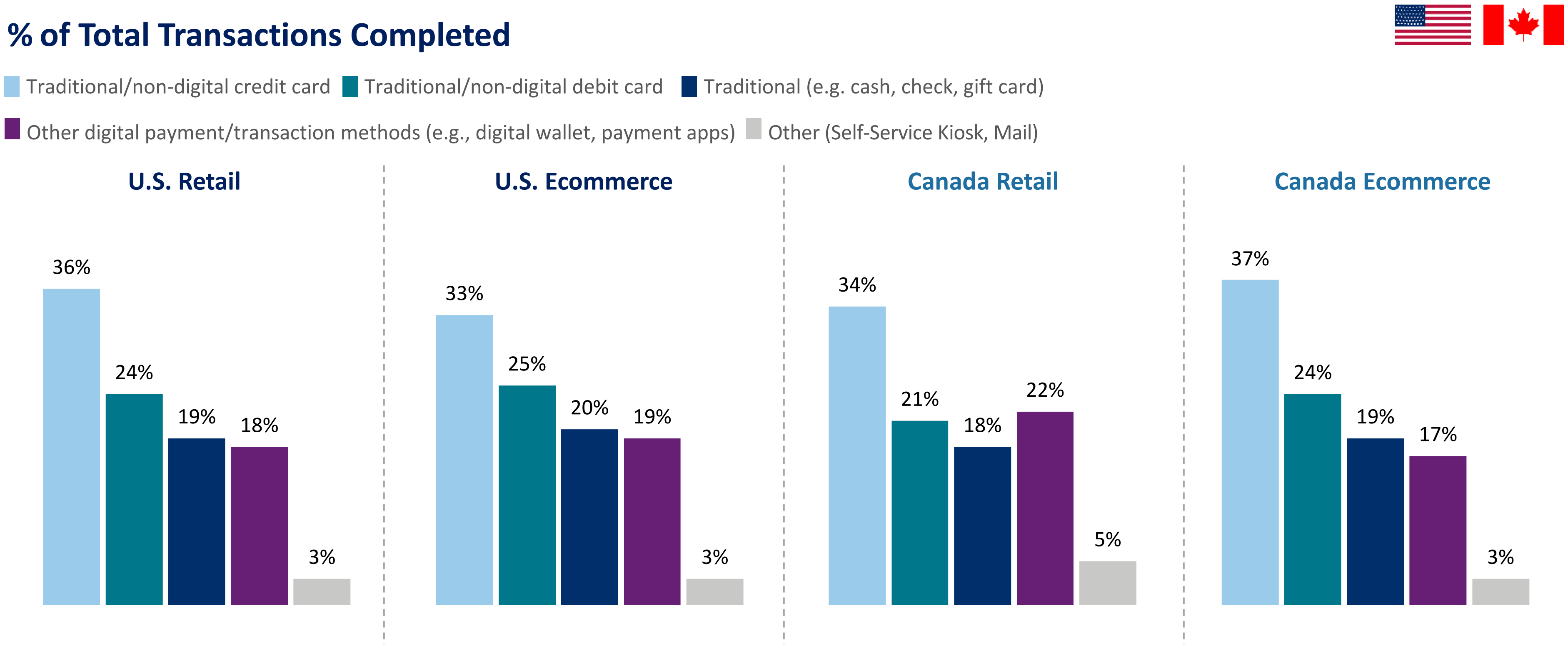
- Digital payments now make up one-fifth of transaction volume.
- Digital transactions drive over half of revenue.
- Digital channels account for 53% of overall fraud losses.

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

Digital payments now make up one-fifth of transaction volume

Payment by digital wallets, payment apps, Buy Now Pay Later (BNPL) schemes and cryptocurrency now account for 21% of merchants' transaction volume.

% of Total Transactions Completed



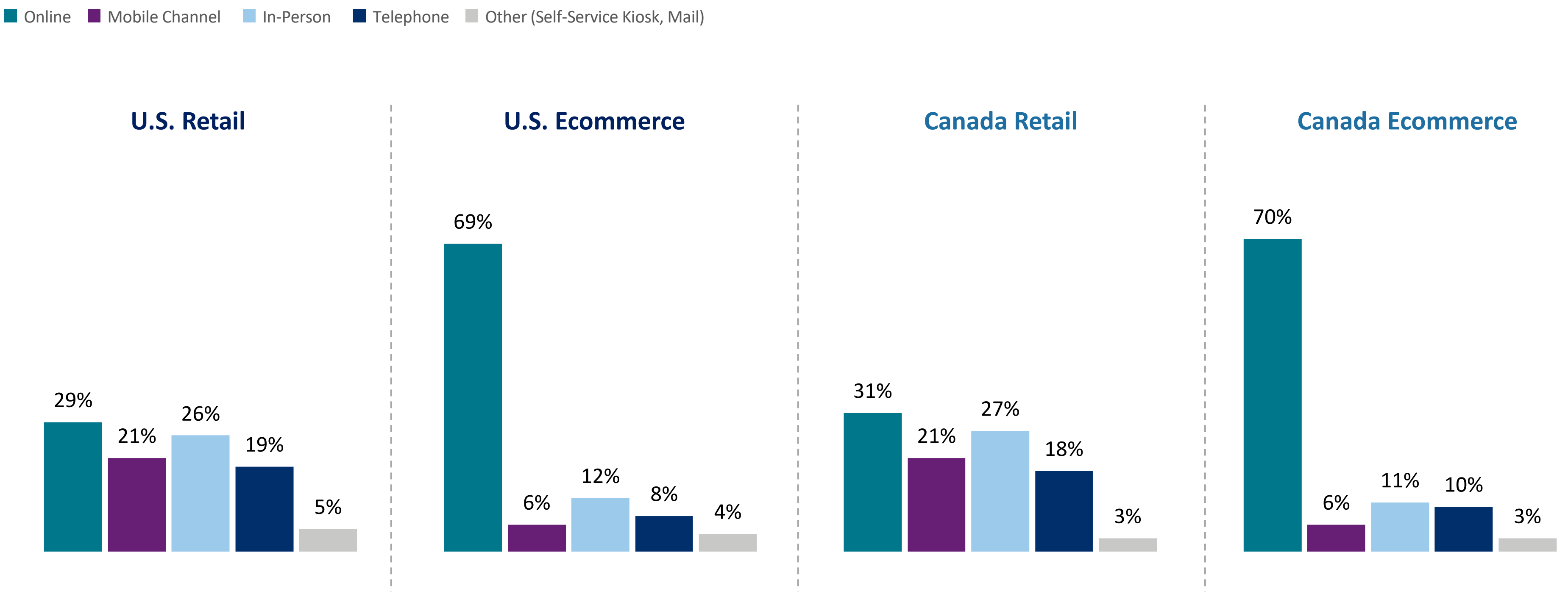
Survey Question:
S7. Using your best estimate, please indicate the percentage of transactions your organization completed during the past 12 months for each of the following payment methods.

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

Digital transactions drive over half of revenue

Consumer behavior indicates an expectation for safe and convenient experiences across all channels.

% of Revenue Attributed to Channel



Survey Question:
S6. Using your best estimate, how does your company's total annual revenue during the past 12 months break out for each of the following channels?

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

More fraud losses occur via digital channels

Fraudsters continue to exploit merchants’ efforts at meeting changing consumer expectations.

Digital Channels Account for 53% of Overall Fraud Losses

DIGITAL CHANNELS

34%
Online

19%
Mobile

NON-DIGITAL CHANNELS

25%
Physical/ In-Store

19%
Telephone/ Contact Center

3%
Other

Survey Question:
Q11. Using your best estimate, please indicate the percent of fraud costs your organization generated through each of the following transaction channels as a percentage of total annual fraud losses.

Key Finding 2

Cybercriminals are seeing more opportunities to exploit both consumers and businesses as adoption of digital services increases in North America and daily life grows more digitized.

- Ecommerce firms face almost 40% more fraudulent transactions than primarily brick-and-mortar retailers.
- Overall fraud levels increase at more than half of merchants.
- Merchants face increasing volumes and varieties of fraud attacks, especially fraudulent chargebacks and identity theft.
- Friendly and first-party fraud are just as common as third-party fraud across the customer journey.
- Scams drive a significant portion of fraud losses, despite efforts to educate consumers. About 34% of fraud losses in the region are now attributed to scams.
- Fraud is driving merchants to increase resource commitment (80% of respondents' organizations), exacerbating financial losses (77%) and impacting customer conversion rates (76%).

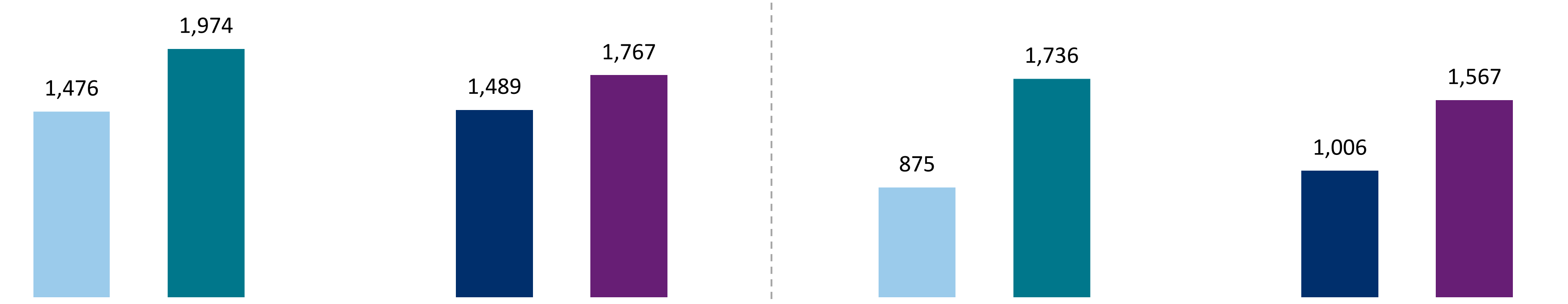
Ecommerce firms face almost 40% more fraudulent transactions than primarily brick-and-mortar retailers

Larger merchants, as well as those with higher ecommerce sales, are particularly prominent targets for fraudsters. Across both the United States and Canada, merchants with a larger digital footprint must protect more attack surface.

Monthly Fraudulent Transactions Completed

Retail | Ecommerce | Small | Mid/Large

U.S.			CANADA		
1,626 fraudulent transactions completed a month	vs	**1,721** fraudulent transactions prevented a month	**1,299** fraudulent transactions completed a month	vs	**1,516** fraudulent transactions prevented a month



Survey Question:
Q14: In a typical month, approximately how many fraudulent transactions does your company prevent?
Q16: In a typical month, approximately how many fraudulent transactions are successfully completed (i.e. not prevented) at your company?

Overview

Key Findings

Digitalization Trends

Attacks and Impacts

Merchant Losses

Challenges Mitigating Fraud

Current Approaches

Recommendations

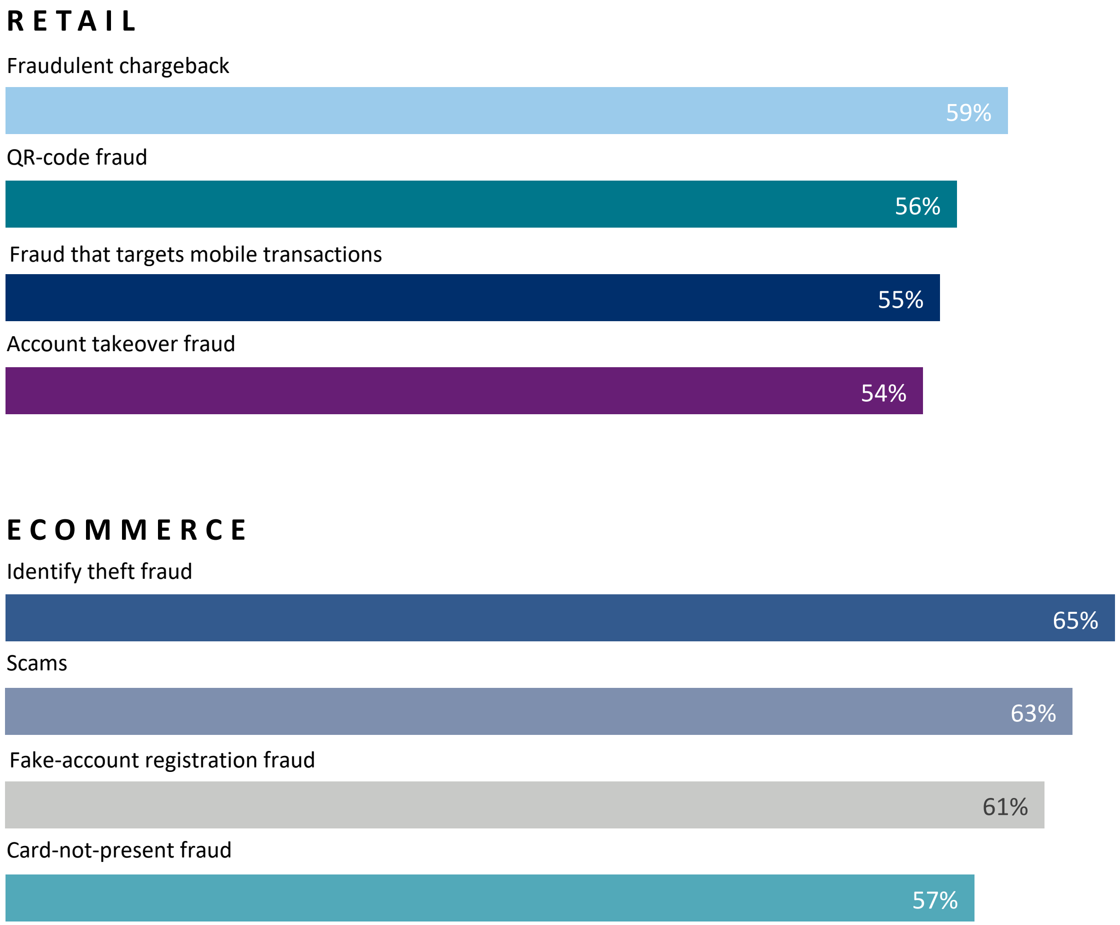
Chargebacks and identity theft lead a multi-faceted assault on merchants

As new types of digital commerce and payment methods have proliferated in North America, transaction fraud has become more frequent and sophisticated. In our survey of 358 fraud management executives at retail organizations in North America, 60% of ecommerce merchants and 53% of retailers report an increase in overall fraud levels.

Retailers are now seeing fraudulent chargebacks as the fastest-growing fraud type, whereas ecommerce merchants note identity theft as the fastest growing fraud type.

Survey Question:
Q2. In the past 12 months, has your company detected less, more, or an equal amount of the following types of online fraud compared to the previous year?

Fastest Growing Fraud Types in Last 12 Months

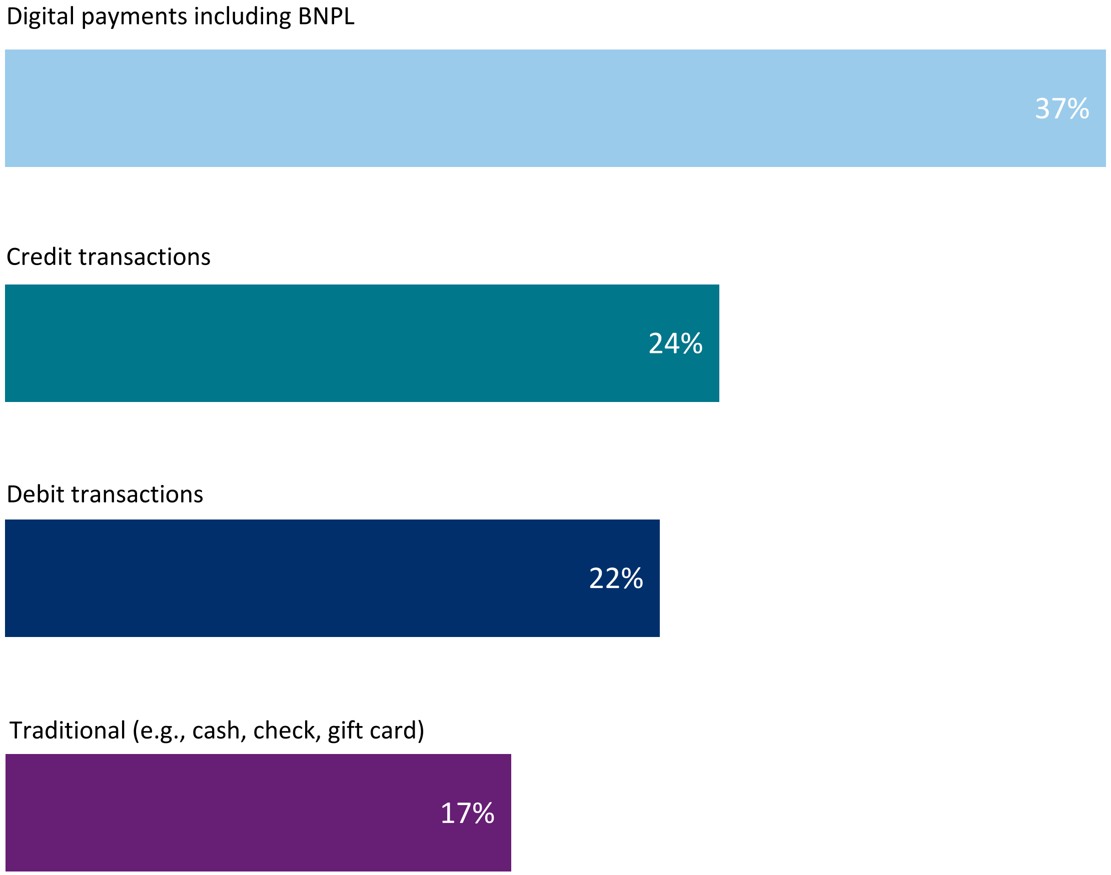


Digital payments and BNPL schemes are particularly vulnerable

Given the increasing frequency and scale of data breaches that compromise consumer data (including card information), as well as their widespread use, credit and debit cards account for the largest share of fraud losses.

That said, merchants also need to pay special attention to digital payments and BNPL transactions. Although relatively new, these transaction methods already make up 37% of fraud losses.

Distribution of Fraud by Transaction Channel



Survey Question:
Q12: Using your best estimate, please indicate the percent of fraud costs your organization generated through each of the following transaction methods as a percentage of total annual fraud losses.

Overview

Key Findings

Digitalization Trends

Attacks and Impacts

Merchant Losses

Challenges Mitigating Fraud

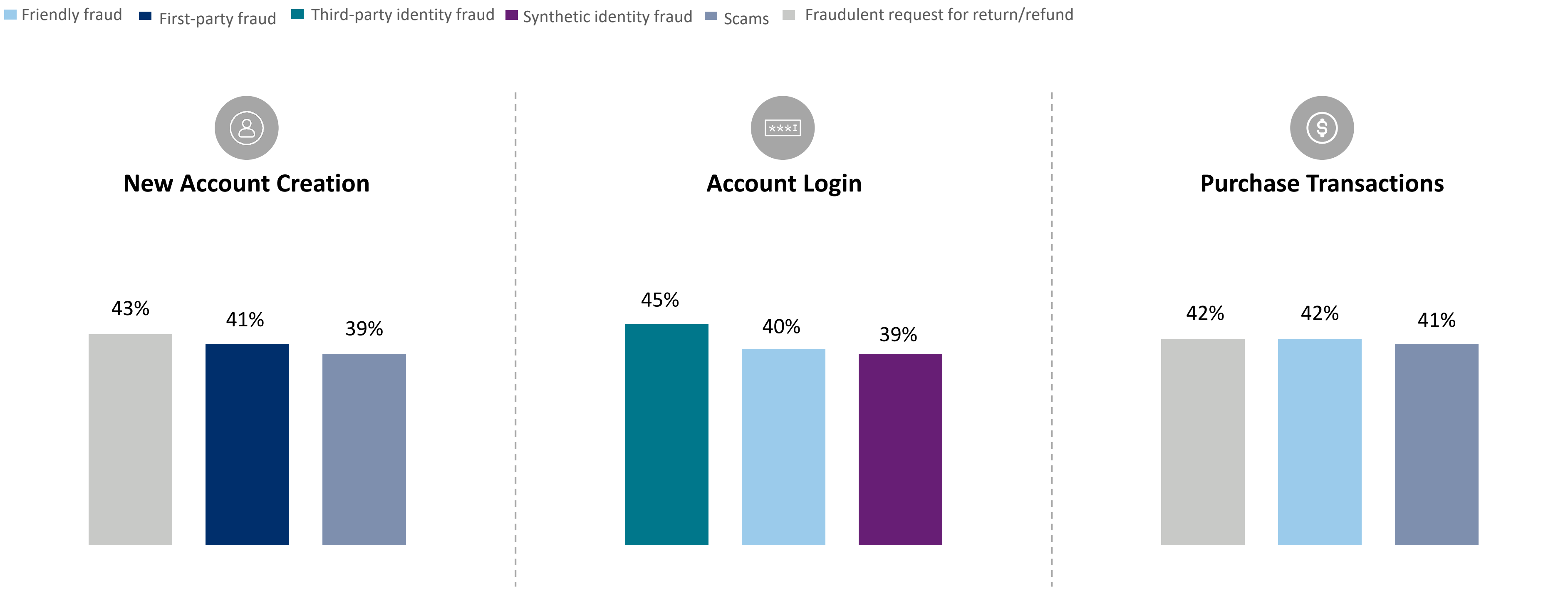
Current Approaches

Recommendations

Friendly and first-party fraud are just as common as third-party fraud

Within the retail and ecommerce sector, businesses have the unique challenge of dealing with both third-party and first-party fraud.

Most Common Fraud Types Observed Along the Customer Journey



Survey Question:
Q8. During the past 12 months, what are the top three types of fraud you have seen in each specific customer-journey stage?

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

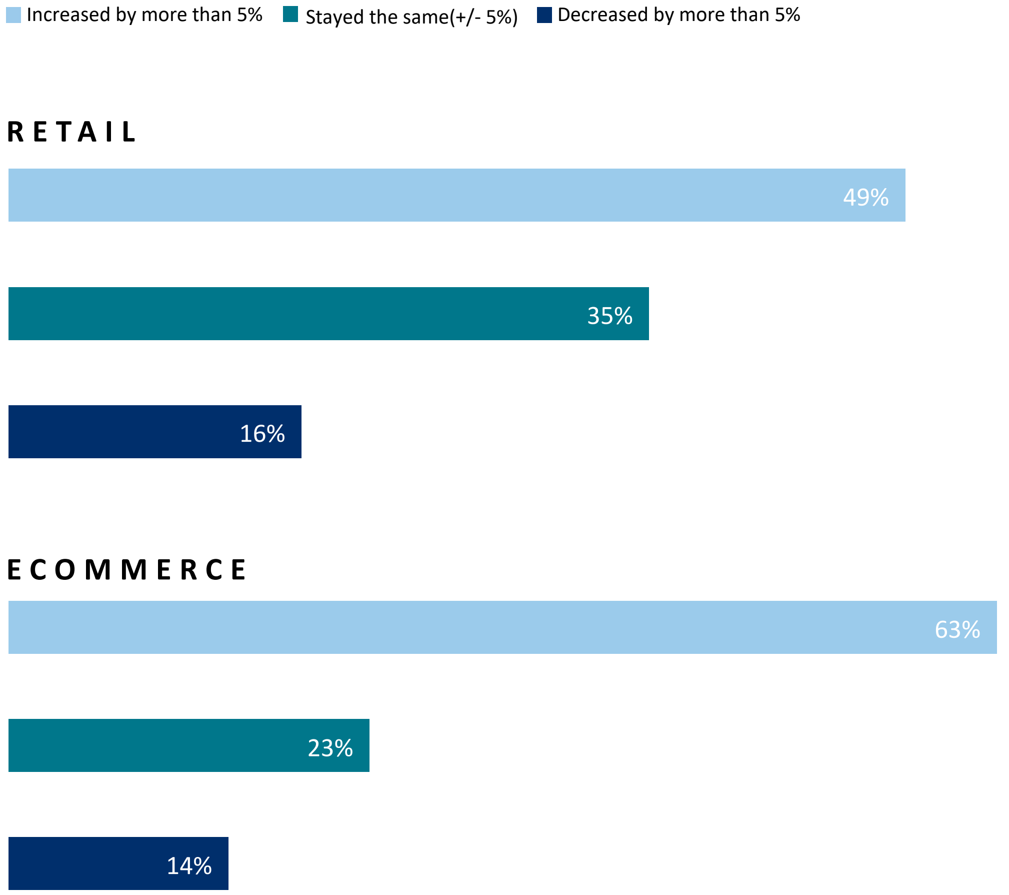
Scams drive a significant portion of fraud losses, despite efforts to educate consumers

Although 46% of merchants surveyed say they have undertaken efforts to educate customers about information security and how to protect themselves against scams, the number of consumers that are falling prey to scammers continue to grow.

Across North America, about half of all merchants report seeing an increase in scams over the last year, with ecommerce merchants more likely to encounter scams.

About 34% of fraud losses in the region are now attributed to scams.

Changing Trends in Scams Over the Past Year



Survey Question:
Q2_15. In the past 12 months, has your company detected less, more, or an equal amount of the following types of online fraud compared to the previous year? — Scams (e.g., consumers manipulated into authorizing transfers against their best interests)
Q5. Of your company's total fraud losses, what percentage of it can be attributed to scams?

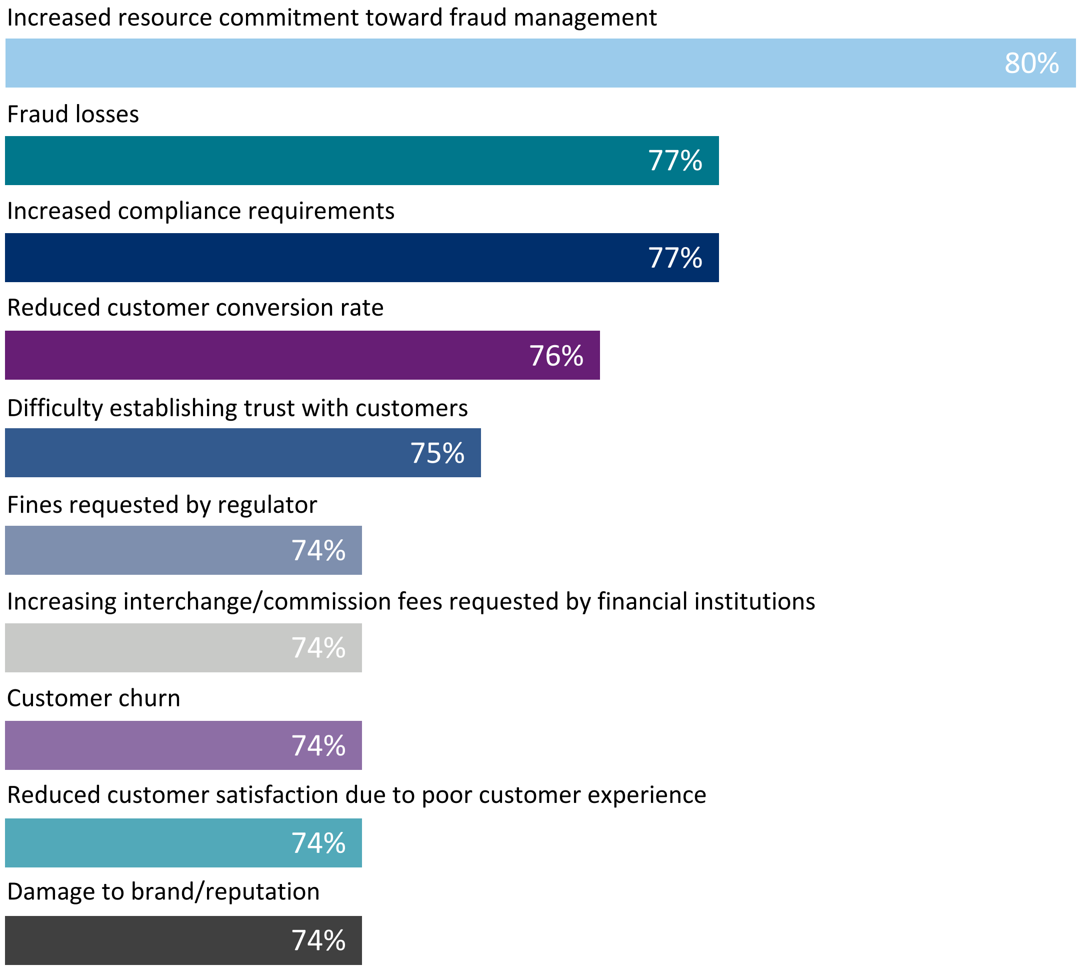
Fraud impacts resources and customer relationships

80% of organizations report that they have had to spend more on fraud management and 77% on fraud losses.

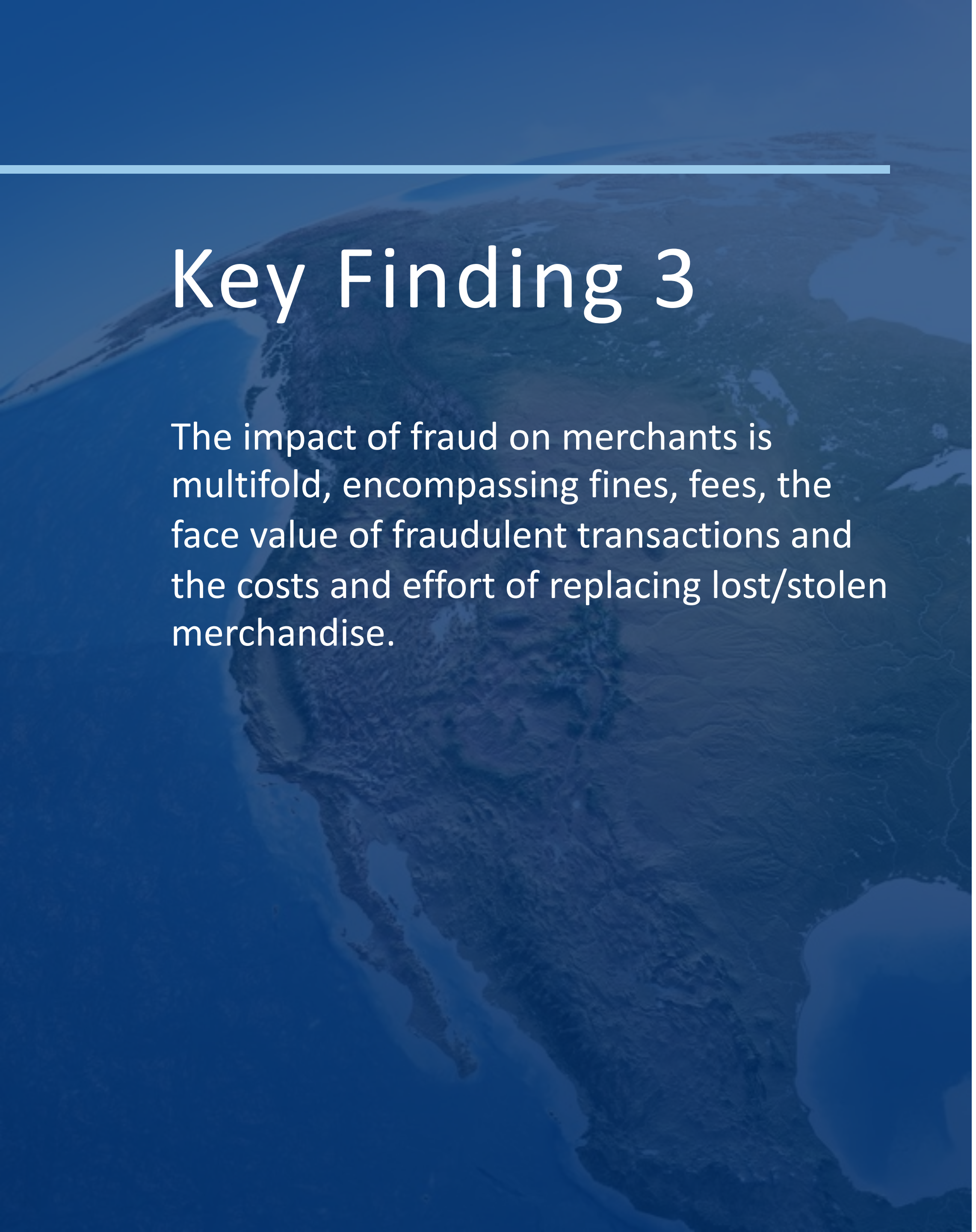
Furthermore, over three-quarters share that conversion rate and customer trust have been negatively impacted. These negative effects can ultimately result in customer churn and financial losses for the company.

Ecommerce businesses are also more affected by compliance requirements and customer experience (CX) than retailers.

Impact of Fraud on Retail and Ecommerce



Survey Question:
Q3. To what extent has fraud impacted the following areas of your business?



Key Finding 3

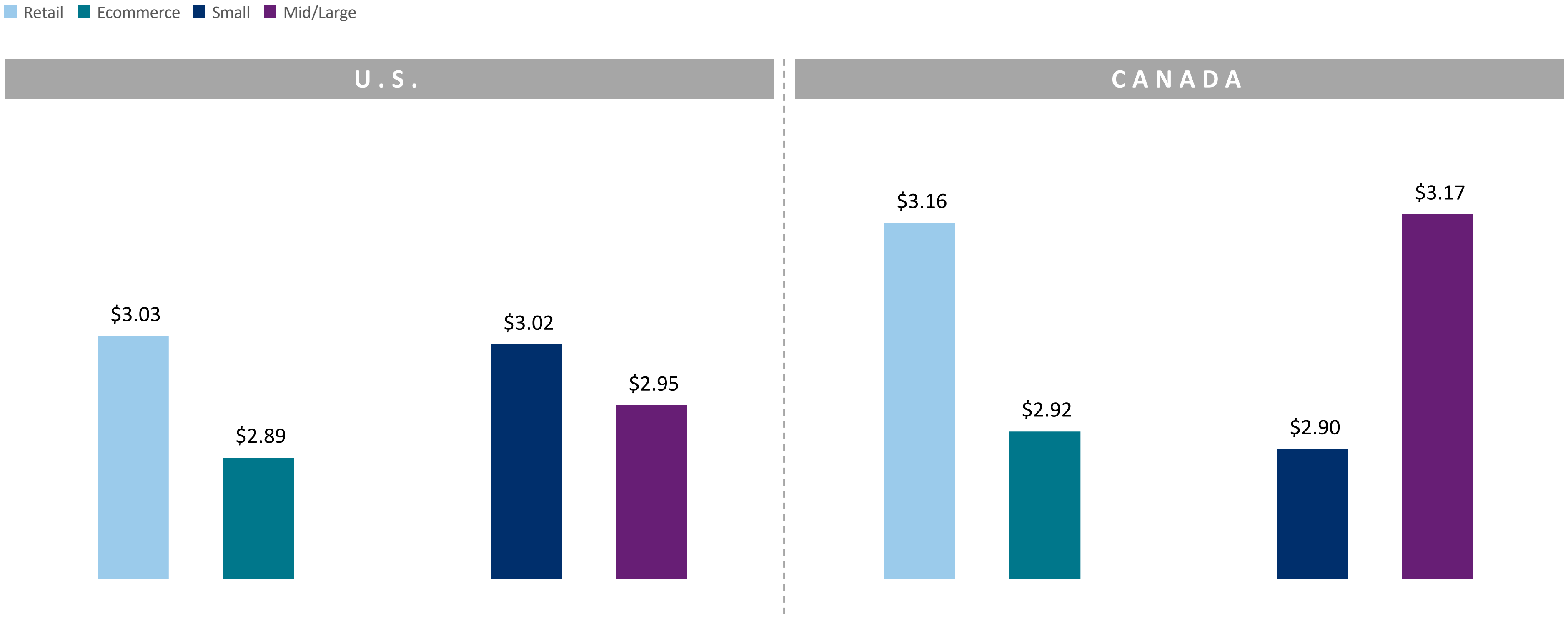
The impact of fraud on merchants is multifold, encompassing fines, fees, the face value of fraudulent transactions and the costs and effort of replacing lost/stolen merchandise.

- Every fraudulent transaction costs 3x the lost transaction value on average, with retailers losing more than ecommerce merchants.
- Nearly half of fraud losses occur at the new account creation stage of the customer journey, even though less than one-third of fraud incidents occur at that stage.
- Card-not-present drives merchant fraud losses.

True Cost Of Fraud™ impact goes far beyond face value lost

Every fraudulent transaction costs 3X the lost transaction value on average. For merchants, this includes the costs of fees and fines, as well as the costs of replacing merchandise.

LexisNexis® Fraud Multiplier™ Cost

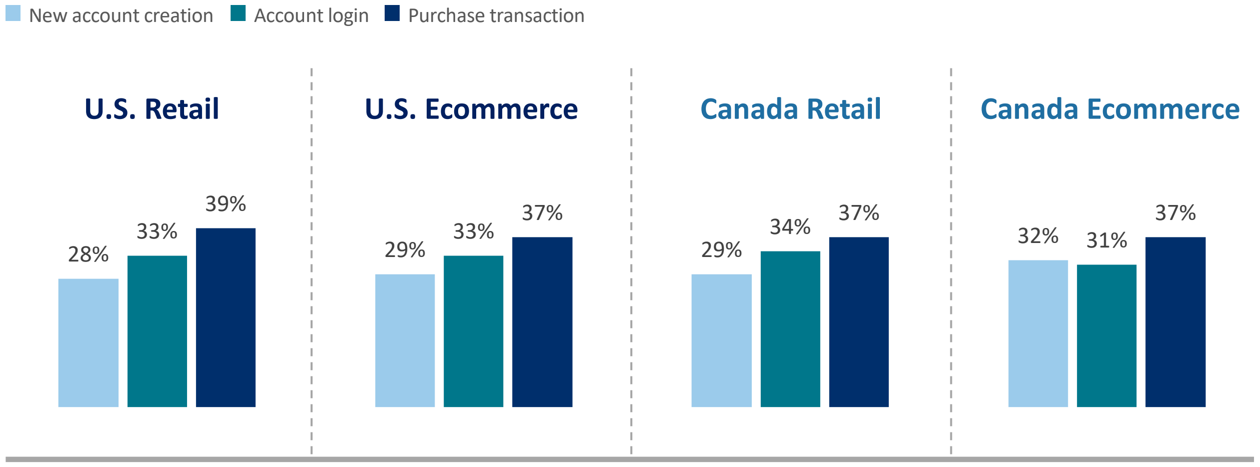


Survey Question:
Q6. In thinking about the total fraud losses suffered by your company, please indicate the distribution of various direct fraud costs over the past 12 months.

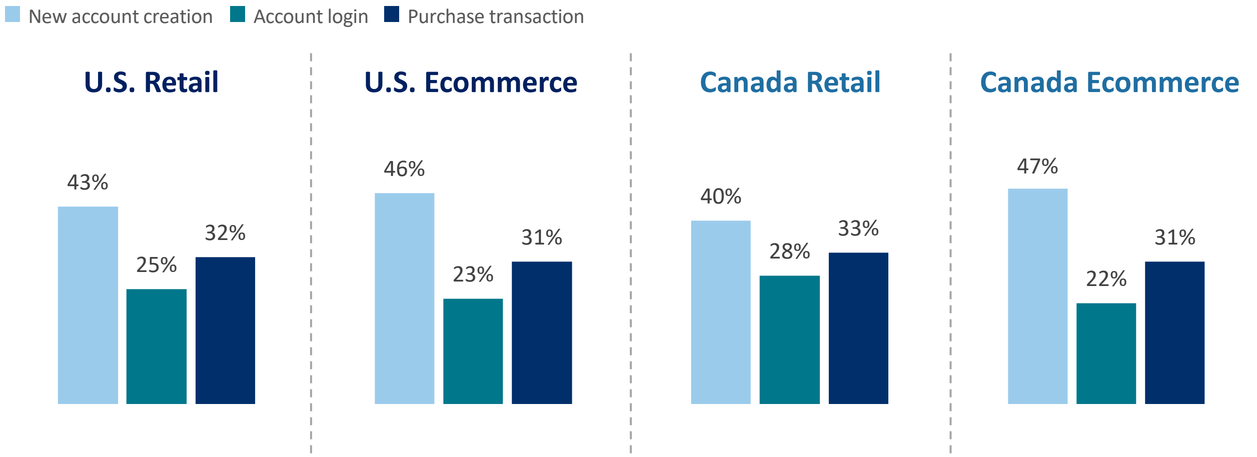
Most fraud losses accrue at new account creation, but more attacks occur at the purchase stage

Given the high growth of identity theft fraud and fake account registration, especially in the ecommerce sector, new account creation also brings the highest risk. Both (physical) retail and ecommerce merchants report that up to 47% of fraud losses can be traced back to this stage in the customer journey, despite lower occurrences overall relative to the other customer journey stages.

Distribution of Fraud Occurrences



Distribution of Fraud Losses

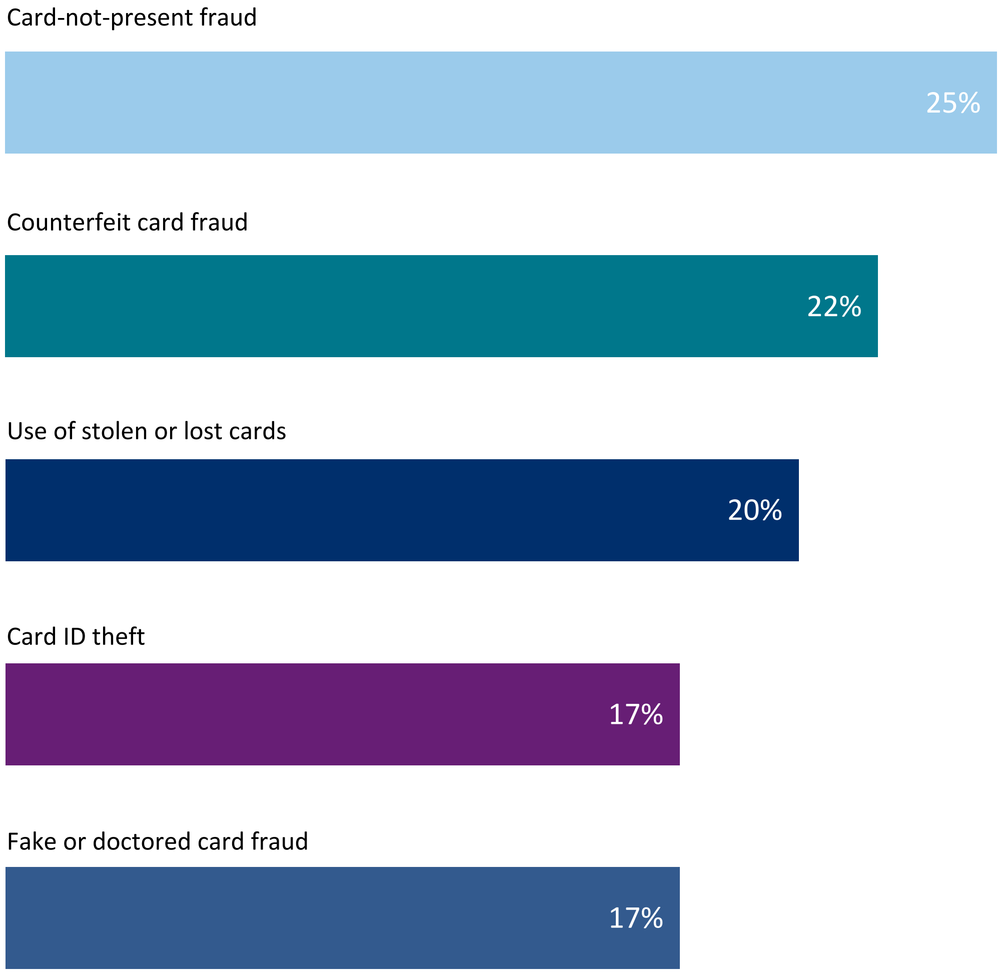


Survey Question:
Q9. For identity-related fraud, what is the distribution by the following types of activities?
Q7. Approximately how much of your organization's fraud losses would you attribute to each of the following customer-journey stages?

Card-not-present drives merchant fraud losses

Challenges with card-related fraud persist because, in part, of difficulties with consumer identity verification.

Distribution of Types of Card Fraud Making Up Credit and Debit-Related Fraud Losses



Survey Question:
Q13. Of your organization's credit- or debit card-related fraud losses, please indicate the distribution across the following types of card fraud.

Key Finding 4

Merchants seek to balance customer safety and customer experience while trying to mitigate new fraud methods and integrate new fraud mitigation capabilities across the customer journey.

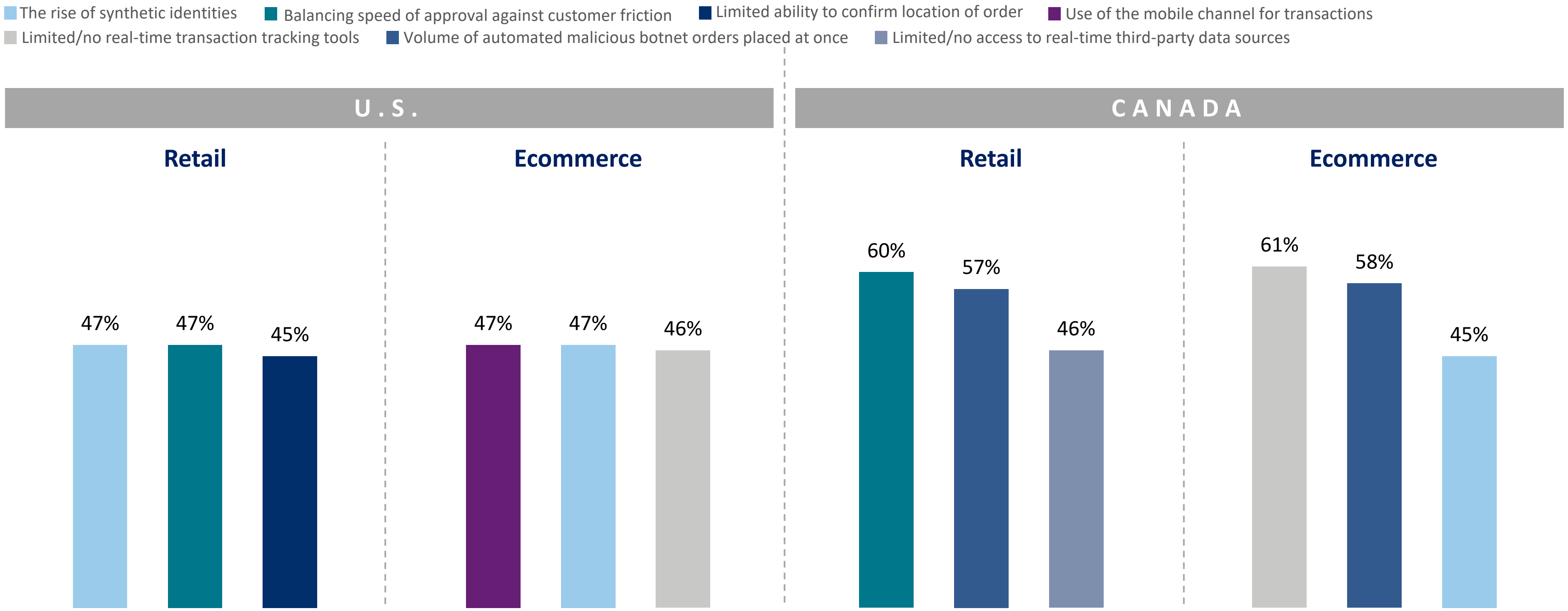
- Efforts to meet changing consumer expectations increases merchant attack surface.
- U.S. merchants report more challenges distinguishing between legitimate human and malicious bot transactions.
- Difficulties verifying customer identity through online channels afflict many merchants.
- Fraud associated with new transaction methods ranks as a top challenge for U.S. merchants.
- Canadian merchants’ online challenges concentrate on determining transaction risk.

Difficulties verifying customer identity afflict many merchants

Fraudsters are becoming more adept at using technologies to advance their crime. Retailers call out the volume of botnet attacks and increased use of synthetic identities as top barriers to customer identity verification.

Factors that Make Customer Identity Verification a Challenge when Serving Customers Through the Online Channel

(Showing rank 1 to 3 in aggregate)



Survey Question:
Q23. Please rank the top three factors that make customer identity verification a challenge when serving customers through the online channel.

New transaction methods increase opportunity for U.S. merchants, but also for fraudsters

In the U.S., both retail and ecommerce merchants rank fraud associated with new transaction methods as a top challenge.

This stems from not understanding what solutions are needed to effectively prevent fraud, and how to implement these technologies.

Survey Question:
Q20. How challenging have these fraud prevention challenges been for your team over the past 12 months?

Main Challenges in Fraud Prevention Over the Past 12 Months

(Showing rank 1 to 5 in aggregate)

RETAIL

1. Managing fraud for new transaction methods
2. Technology implementation complexity
3. Staying current and defending against new, more sophisticated payment frauds

ECOMMERCE

1. Difficulty understanding what solution(s) are needed
2. Balancing fraud-prevention friction with customer experience
3. Managing fraud for new transaction methods

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

U.S. merchants report the most online challenges with bots, friction and identity verification

Across the customer journey, malicious bot transactions were a top-three challenge for more U.S. merchants than any other issue. Ecommerce merchants report struggles with identity verification at all stages. Merchants remain sensitive to balancing fraud-prevention friction with the customer experience, particularly in the purchase stage of the customer journey.

Top Three Ranked Online Fraud Challenges

	New Account Creation		Account Login		Purchase Transactions	
	Retail	Ecommerce	Retail	Ecommerce	Retail	Ecommerce
IDENTITY						
Verification – Email or Device	26%	28%	24%	22%	28%	23%
Verification – Identity	26%	41% ▲	27%	31% ▲	25%	37% ▲
Verification – Phone	23%	26%	24%	30%	29%	31%
Verification – Address	27%	30%	22%	31% ▲	26%	30%
TRANSACTION						
Knowing origination source	32% ▲	22%	29%	23%	27%	20%
Lack of specialized tools*	26%	29%	25%	26%	27%	32% ▲
New transaction methods	26%	24%	26%	18%	27%	26%
IMPACTS						
Malicious bot transactions**	32% ▲	37% ▲	34% ▲	41% ▲	30% ▲	29%
Assessing risk by country	30%	23%	30%	28%	23%	21%
Manual reviews	26%	17%	29%	24%	28%	20%
Balancing fraud-prevention friction***	27%	23%	32% ▲	25%	31% ▲	32% ▲

Survey Question:
Q21. Please rank the top three challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE channel.

▼▲ = most notable challenge per industry segment per customer journey stage

* "Lack of specialized tools" = Lack of specialized fraud prevention tools for international transactions
** "Malicious bot transactions" = Inability to distinguish between legitimate human and malicious bot transactions
*** "Balancing fraud-prevention friction" = Balancing fraud-prevention friction with the customer experience

U.S. merchants grapple with identity challenges across the mobile customer journey

Malicious bot transactions also rank high across new account creation and account login interactions.

Top Three Ranked Mobile Fraud Challenges

	New Account Creation		Account Login		Purchase Transactions	
	Retail	Ecommerce	Retail	Ecommerce	Retail	Ecommerce
IDENTITY						
Verification – Email or Device	29% ▲	22%	26%	27%	23%	32%
Verification – Identity	23%	23%	30% ▲	39% ▲	29%	32%
Verification – Phone	28%	30%	26%	34% ▲	30% ▲	32%
Verification – Address	32% ▲	33% ▲	26%	25%	26%	35% ▲
TRANSACTION						
Knowing Origination Source	28%	27%	29%	30%	25%	34% ▲
Lack of specialized tools*	24%	32%	26%	16%	25%	20%
New Transaction Methods	28%	28%	25%	29%	29%	19%
IMPACTS						
Malicious bot transactions**	29% ▲	33% ▲	32% ▲	33%	25%	33%
Assessing risk by country	26%	27%	27%	24%	31% ▲	22%
Manual reviews	28%	19%	26%	19%	29%	19%
Balancing fraud-prevention friction***	25%	28%	27%	23%	30% ▲	23%

Survey Question:
Q22. Please rank the top three challenges in each customer-journey stage related to fraud your company faces when serving customers using the MOBILE channel.

▼▲ = most notable challenge per industry segment per customer journey stage

* "Lack of specialized tools" = Lack of specialized fraud prevention tools for international transactions

** "Malicious bot transactions" = Inability to distinguish between legitimate human and malicious bot transactions

*** "Balancing fraud-prevention friction" = Balancing fraud-prevention friction with the customer experience

Canadian merchants seek to balance customer protection and experience

In Canada, retail companies are facing difficulties protecting their customers while providing a good customer experience.

Ecommerce merchants are challenged by the lack of customer education regarding those threats, and struggle to fight against new fraud technologies.

Main Challenges in Fraud Prevention Over the Past 12 Months

(Showing rank 1 to 5 in aggregate)

RETAIL

1. Balancing fraud-prevention friction with customer experience
2. Technology implementation complexity
3. Regulatory/compliance issues or concerns

ECOMMERCE

1. Lack of consumer education
2. Staying current and defending against new, more sophisticated payment frauds
3. Distinguishing between legitimate human and malicious bot transactions

Survey Question:
Q20. How challenging have these fraud prevention challenges been for your team over the past 12 months?

Canadian merchants’ online challenges concentrate on determining transaction risk

Ecommerce merchants indicated inability to determine transaction source/origin as a primary challenge across the customer journey. Retailers struggle balancing fraud-prevention friction with the customer experience, and the emergence of new/varied transaction methods.

Top Three Ranked Online Fraud Challenges

	New Account Creation		Account Login		Purchase Transactions	
	Retail	Ecommerce	Retail	Ecommerce	Retail	Ecommerce
IDENTITY						
Verification – Email or Device	17%	24%	29%	41% ▲	26%	21%
Verification – Identity	14%	21%	11%	32%	23%	26%
Verification – Phone	26%	21%	29%	21%	20%	38% ▲
Verification – Address	17%	26%	29%	26%	11%	15%
TRANSACTION						
Knowing Origination Source	29%	41% ▲	37% ▲	38% ▲	31%	44% ▲
Lack of specialized tools*	23%	35% ▲	31%	21%	11%	32%
New Transaction Methods	37% ▲	35% ▲	26%	26%	43% ▲	21%
IMPACTS						
Malicious bot transactions**	31%	24%	20%	32%	49% ▲	32%
Assessing risk by country	29%	26%	26%	21%	31%	29%
Manual reviews	23%	21%	29%	15%	26%	9%
Balancing fraud-prevention friction***	54% ▲	26%	34% ▲	25%	29%	32%

Survey Question:
Q21. Please rank the top three challenges for each customer journey stage related to fraud your company faces when serving customers using the ONLINE channel.

* "Lack of specialized tools" = Lack of specialized fraud prevention tools for international transactions
** "Malicious bot transactions" = Inability to distinguish between legitimate human and malicious bot transactions
*** "Balancing fraud-prevention friction" = Balancing fraud-prevention friction with the customer experience

▼▲ = most notable challenge per industry segment per customer journey stage

Canadian merchants struggle to balance fraud-prevention friction with customer experience

Retailers concentrate on the account login stage of the mobile customer journey.

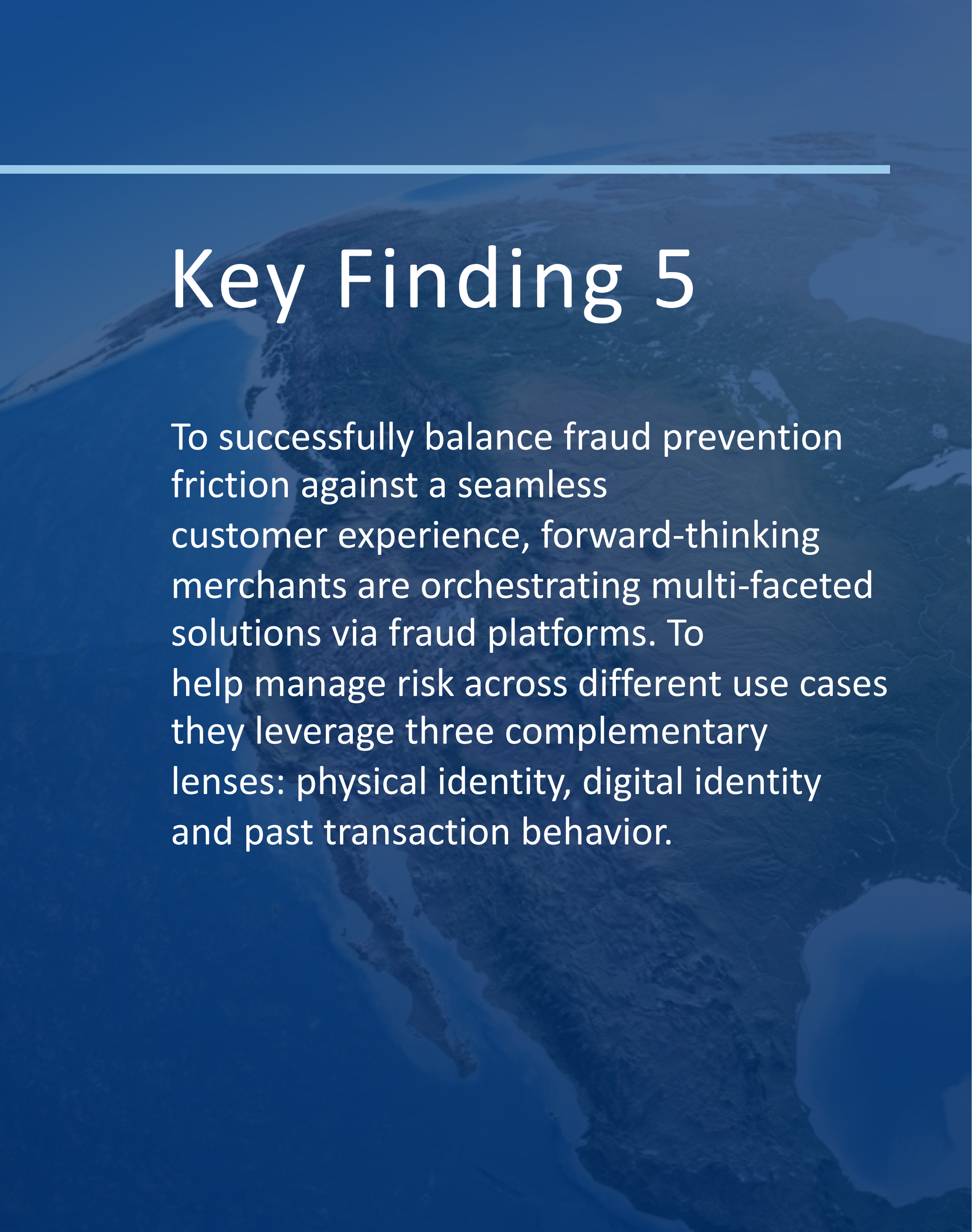
Top Three Ranked Mobile Fraud Challenges

	New Account Creation		Account Login		Purchase Transactions	
	Retail	Ecommerce	Retail	Ecommerce	Retail	Ecommerce
IDENTITY						
Verification – Email or Device	34%	26%	29%	35% ▲	20%	26%
Verification – Identity	31%	19%	23%	26%	29%	26%
Verification – Phone	26%	29%	20%	26%	31%	35% ▲
Verification – Address	26%	26%	26%	23%	26%	35% ▲
TRANSACTION						
Knowing Origination Source	31%	32%	14%	29%	20%	26%
Lack of specialized tools*	9%	35% ▲	34% ▲	26%	14%	23%
New Transaction Methods	34% ▲	16%	46% ▲	23%	26%	32%
IMPACTS						
Malicious bot transactions**	31%	23%	34% ▲	26%	37% ▲	19%
Assessing risk by country	40% ▲	26%	34% ▲	26%	29%	29%
Manual reviews	26%	32%	14%	29%	29%	19%
Balancing fraud-prevention friction***	11%	35% ▲	26%	32% ▲	40% ▲	29%

Survey Question:
Q22. Please rank the top three challenges in each customer-journey stage related to fraud your company faces when serving customers using the MOBILE channel.

▲ = most notable challenge per industry segment per customer journey stage

* "Lack of specialized tools" = Lack of specialized fraud prevention tools for international transactions
** "Malicious bot transactions" = Inability to distinguish between legitimate human and malicious bot transactions
*** "Balancing fraud-prevention friction" = Balancing fraud-prevention friction with the customer experience



Key Finding 5

To successfully balance fraud prevention friction against a seamless customer experience, forward-thinking merchants are orchestrating multi-faceted solutions via fraud platforms. To help manage risk across different use cases they leverage three complementary lenses: physical identity, digital identity and past transaction behavior.

- Over two-thirds (69%) of merchants report integrating fraud prevention with customer experience.
- Adoption of risk signals varies between merchants, though location analysis and threat detection are the most common.
- Across industries, geographies and customer journey stages, there remains ample opportunity for integrating multi-tiered solutions across the customer journey.
- When considering upgrades, merchants prioritize fraud management administration capabilities, and models that incorporate machine learning.
- Over two-thirds (69%) of merchants expect to increase spending on fraud prevention over the next 12 months.

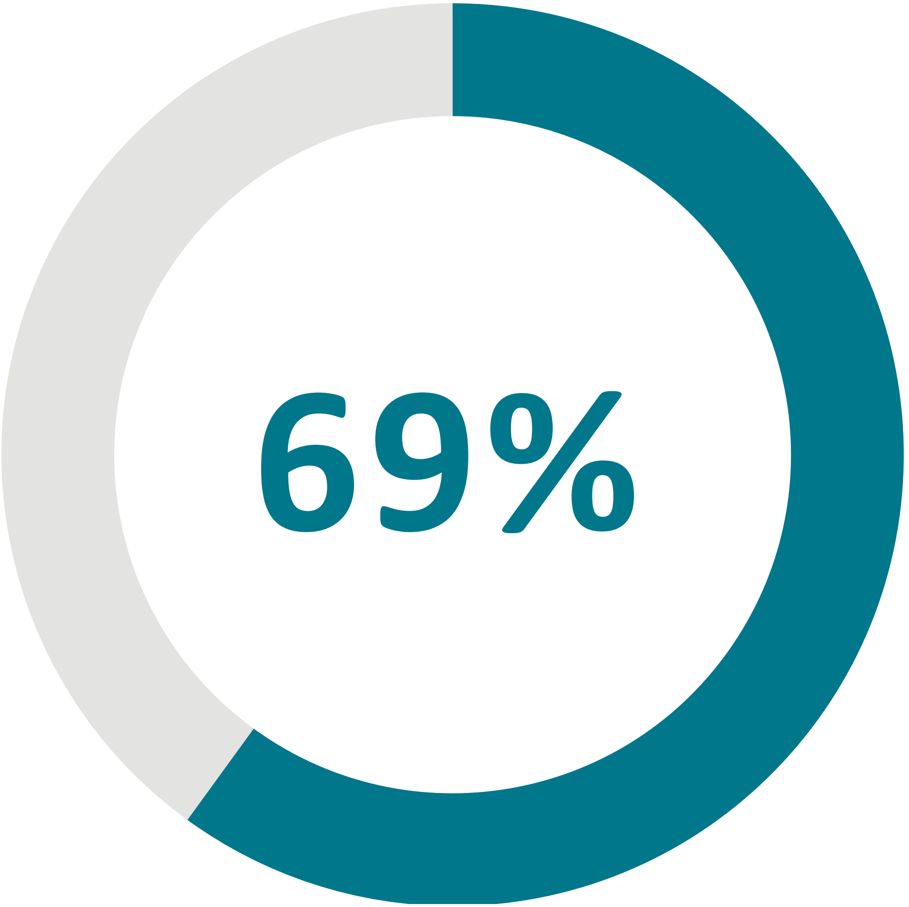
Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

Many merchants report integrating fraud prevention with customer experience

Organizations need an integrated approach to managing fraud and customer experience in order to balance the priorities of both mandates.

For now, 69% say they have integrated digital/customer experience operations with fraud-prevention efforts.

Integrated Digital/Customer Experience Operations

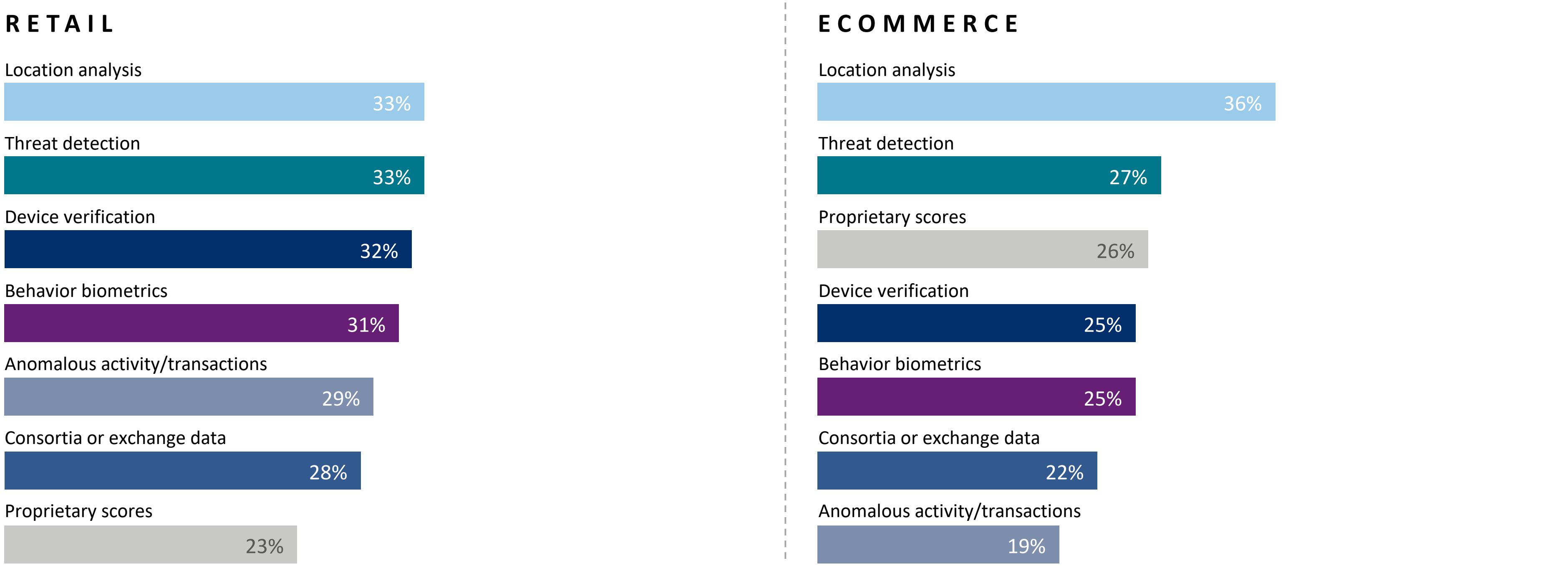


Survey Question:
Q19. How much do you agree with the following statements? - My organization has integrated its digital/customer experience operations with fraud-prevention efforts.

Different merchants adopt different risk signals

Proactively scoring events and transactions can help minimize customer friction by eliminating unnecessary verification processes for legitimate customers, and help organizations reduce cost of managing fraud. However, only 64% of merchant organizations currently have a fraud-risk scoring model governance process and supporting tool in place.

Risk Signals Methods Used By Organizations



Survey Question:
Q18. Which of the following risk signals methods does your organization use?

Fraud management administration and AI/ML models usage top the list of desired solution features

Retailers and ecommerce businesses are seeking service providers who can deliver advanced features and technologies.

A more comprehensive fraud management administration and utilization of AI/ML models are key for both. Having robust fraud management administration capabilities is key for both financial services and lending firms, as this empowers administrators to effectively configure, monitor, and maintain the fraud management system. Other features include card-payment fraud models and account takeover detection.

RETAIL

1. Fraud-management-administrator management
2. AI and ML models usage
3. Card-payment fraud models

ECOMMERCE

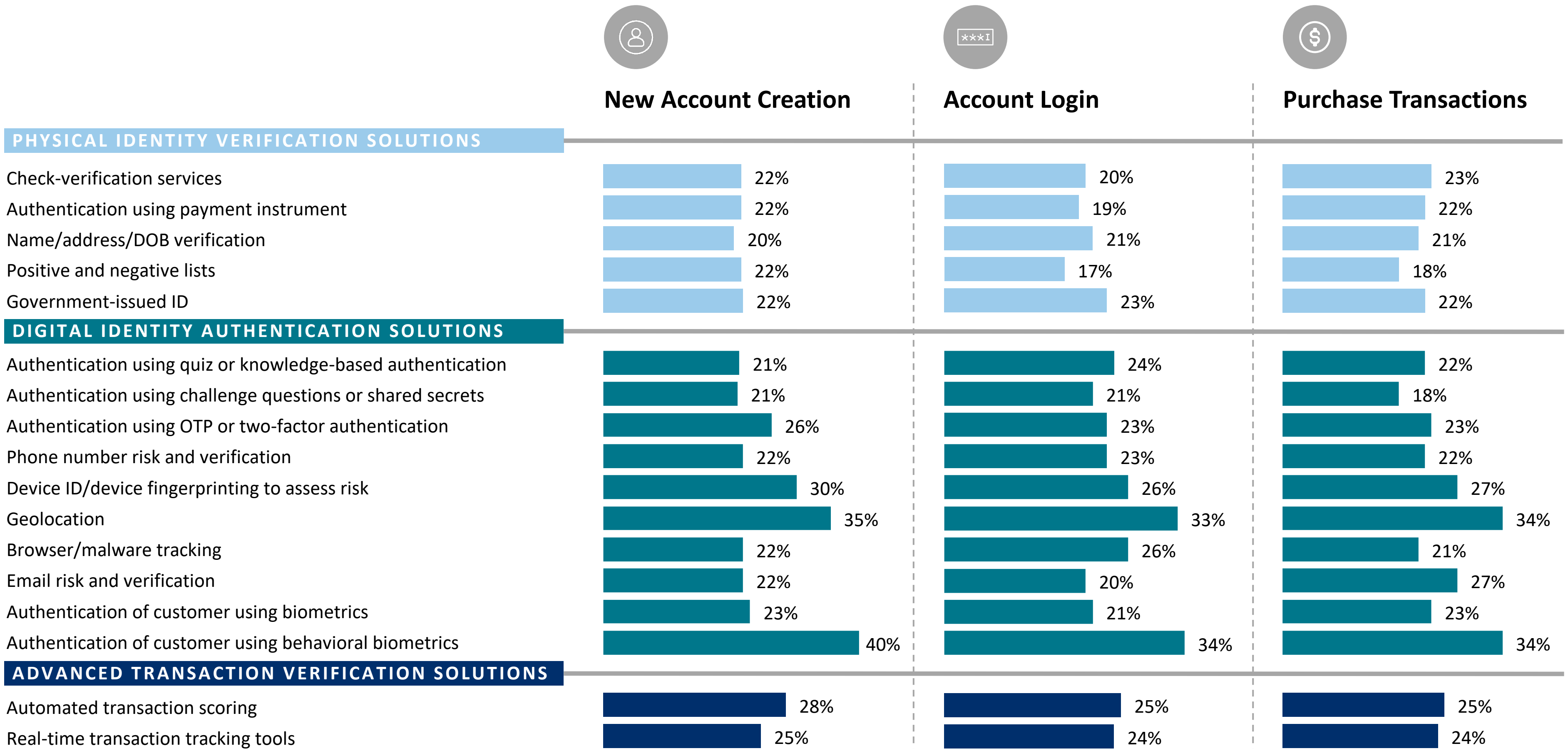
1. Fraud-management-administrator management
2. AI and ML models usage
3. Account-takeover detection

Survey Question:
Q28. What are the top five most important features in a fraud-management solution?

Ample opportunity remains for multi-tiered solutions along the customer journey

As fraud can take many forms, and evolves continuously, organizations need a comprehensive approach to fraud detection and prevention. Although merchants report implementing some solutions, adoption rates indicate room for growth.

Adoption of Fraud Mitigation Solutions Across the Customer Journey



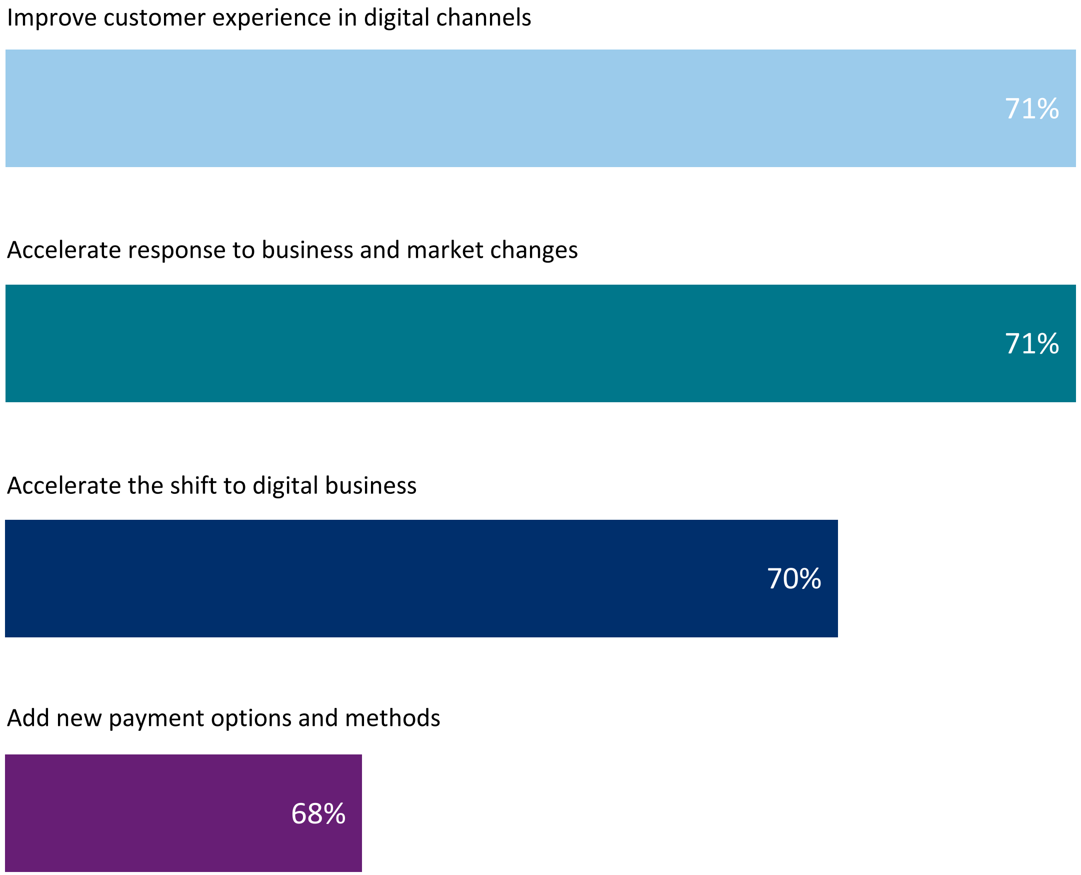
Survey Question:
Q24. Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer-journey points?

Organizations need to prioritize risk-based fraud management to keep apace of digitalization

With ecommerce predicted to continue increasing over the next few years,* consumers will also increase engagement with new digital channels and adopt new digital payment methods. This further increases the likelihood of fraud, creating more urgency for organizations to build an effective fraud mitigation plan in place.

Prioritization of Various Initiatives Over the Next 12 Months

(Showing “critical priority” and “high priority” in aggregate)



Survey Question:
Q1. To what extent is your organization prioritizing the following business initiatives during the next 12 months?

* Source: "US Online Retail Forecast, 2023 - 2028," Forrester Research, Inc., July 20, 2023.

Retailers are ready to invest in additional fraud solutions

Retailers are committed to integrate digital and customer experience operations within their fraud prevention efforts.

To that end, they are looking into fraud solutions that minimize customer friction during authentication, and 69% expect to increase their spending on fraud prevention over the next 12 months.

They are interested in increasing investments into biometrics authentication methods, automated transaction scoring and malware tracking.

RETAIL

1. Authentication of customer using biometrics
2. Automated transaction scoring
3. Geolocation

ECOMMERCE

1. Authentication of customer using biometrics
2. Browser/malware tracking
3. Email risk and verification

Survey Question:
Q25. Which of the following fraud solutions, if any, does your company expect to invest in during the next 24 months?

Recommendations

To respond faster to emerging fraud trends and rising consumer expectations, merchants must take a dynamic and agile approach to risk assessment. Capabilities integrated via risk-based workflows, supported by deep troves of identity intelligence and robust linking technology promote the flexibility necessary for safer and more convenient interactions and transactions.

- To minimize impact on low-risk transactions and legitimate customers, calibrate and apply anti-fraud measures based on the level of risk associated with each transaction or customer via a risk-based, data-driven approach to fraud management.
- To support customer acquisition and retention, strike a balance between fraud management and customer experience by leveraging solutions that perform without active consumer engagement.
- Work with vendors leveraging emerging technologies that can enable more efficient data sharing and collaboration across internal divisions.
- Organizations that build a more robust posture against fraud throughout customer journey stages report 46% lower fraud losses compared to the least mature organizations.

Recommendation #1

Combine a risk-based and data-driven approach to fraud management. To better identify patterns and anomalies in customer behavior, use advanced data analytics tools and techniques. Calibrate and apply anti-fraud measures based on the level of risk associated with each transaction or customer to minimize impact on low-risk transactions and legitimate customers.

Protect Entry Points

Implement strong customer identity and access management (CIAM) controls by starting with integrating cybersecurity and digital experience operations with fraud detection technology. This helps to guard against attacks while optimizing the customer experience.

Breached data used to access accounts requires more levels of security to distinguish a legitimate consumer from a bot or synthetic identity.

MULTI-LAYERED SOLUTIONS APPROACH

Authenticate the Digital Person to Distinguish Between Legitimate and Fake Customers/Fraudsters

Analyze signals from digital interactions, including device usage, device reputation and digital identifiers, to discern between legitimate users and potential fraud risks. This is particularly important at account login since fraudsters deploy mass attacks using breached data to test passwords for account takeover. Leverage crowdsourced device and account intelligence for additional risk signal.

Solution examples: authentication by biometrics; email/phone risk assessment – seamless risk assessment that minimizes customer effort and friction

Authenticate the Device

Identify a remote computing device or user.

Solution examples: device ID/ fingerprint; geolocation

Active Identity Authentication

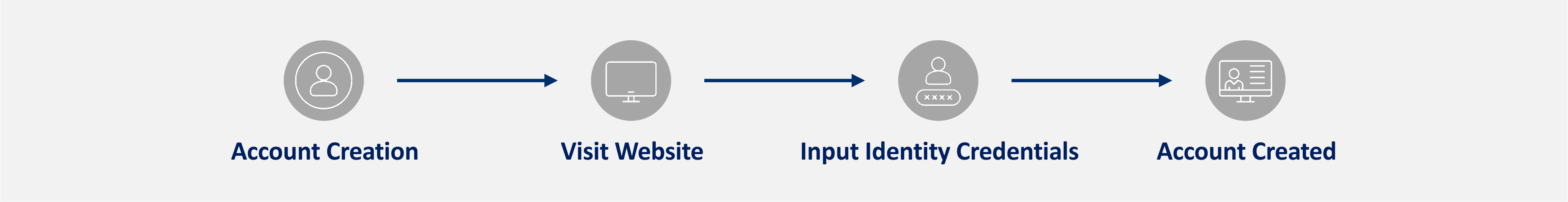
Confirm the user's claimed identity via personal data known only to the customer or via a physical device in the user's possession.

Solution examples: authentication by challenge, quiz or shared secrets; authentication using OTP/2 factor

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

Recommendation #2

Balance fraud management effectiveness and customer experience. As digital interactions and transactions become increasingly common, businesses are competing intensively to win and retain new customers; therefore, customer onboarding and payment journeys should be as seamless as possible.



MULTI-LAYERED SOLUTIONS APPROACH

Protect Entry Points

Implement strong customer identity and access management (CIAM) controls by integrating cybersecurity and digital experience operations with fraud detection technology. This helps to guard against attacks while improving the customer experience.

Authenticate the Physical Person

Verify physical identity attributions
Solution examples: name/address/ DOB verification

Authenticate the Digital Person

Analyze signals from digital interactions, including device usage, device reputation and digital identifiers, to discern between legitimate users and potential fraud risks.

Solution Examples: Authentication by behavioral biometrics; email/ phone risk assessment; *Device ID/fingerprint – seamless risk assessment that minimizes customer effort*

Continue to manage risk across all endpoints

Increase flexibility and reduce complexity via a robust and interoperable array of physical, digital and behavioral risk and authentication assessment capabilities.

To strike a balance between fraud management effectiveness and customer experience, leverage solutions that perform without active consumer engagement, such as behavioral biometric-based risk assessments.

Overview

Key Findings

Digitalization Trends

Attacks and Impacts

Merchant Losses

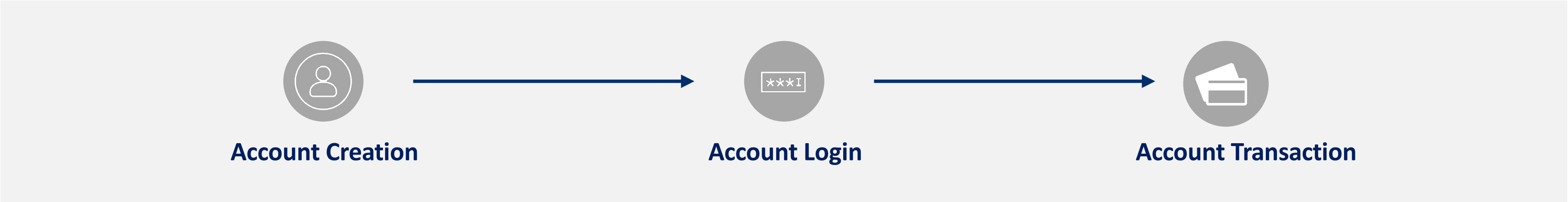
Challenges Mitigating Fraud

Current Approaches

Recommendations

Recommendation #3

Work with vendors leveraging emerging technologies. AI/ML-based technologies including supervised learning, unsupervised learning, deep learning and graph computing have become the norm in fraud management. Richer data insights into fraud analysis can break down data silos across divisions and organizations and enable more efficient data sharing.



Account Creation

Account Login

Account Transaction

- ✓ Single point protection is no longer enough and results in single point of failure.
- ✓ As consumers transact across locations, devices, and geographies, user behaviors, such as transaction patterns, payment amounts, and payment beneficiaries, are becoming more varied and less predictable.
- ✓ Adoption among consumers of more online and mobile transactions means that more transactions are occurring in an anonymous environment compared to traditional in-person interactions. Assessing only the physical identity attributes (name, address, date of birth, Social Security Number, etc.) won’t help businesses to authenticate the identity. Businesses need to also assess the device risk, online/mobile behaviors and transaction risk.
- ✓ Further, each stage of the customer journey is a unique interaction, requiring different types of identity assessment, data and solutions to let customers in and keep fraudsters out.
- ✓ A multi-layered, strong authentication defense approach is needed. This includes a single authentication decision platform that incorporates real-time event data, third-party signals and global, cross-channel intelligence.
- ✓ Using valuable data attributes like users’ login from multiple devices, locations, and channels is essential for identifying risks and mitigating more account takeover attacks.
- ✓ Enabling integrated forensics, case management, and business intelligence can help to improve productivity.

Overview
Key Findings
Digitalization Trends
Attacks and Impacts
Merchant Losses
Challenges Mitigating Fraud
Current Approaches
Recommendations

Layered solutions help prevent more fraud

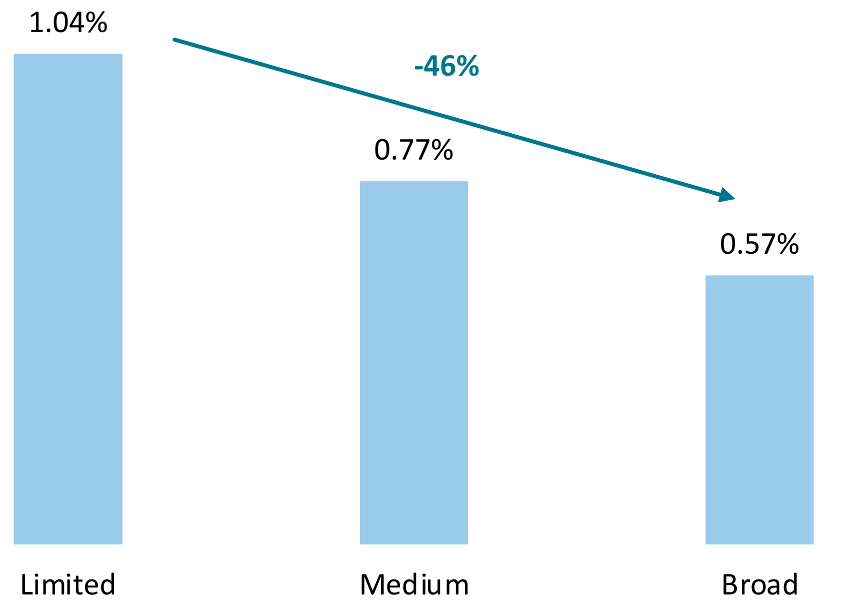
Smart investments in varied solutions pay off: organizations that build a more robust posture against fraud throughout customer journey stages report lower fraud losses.

Fraud Losses (as Percent of Revenue), by Strength of Fraud Prevention Measures

-46%

Difference in fraud loss of most mature vs. least mature organizations

Range of solutions implemented across the three customer journey stages.



LexisNexis® Risk Solutions can help.

For more information:

risk.lexisnexis.com/FIM

+1-800-953-2877
+408-200-5755

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data, sophisticated analytics platforms and technology solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

This document is for informational purposes only. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

LexisNexis®
RISK SOLUTIONS

This document is for informational purposes only. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.