LexisNexis®
RISK SOLUTIONS

LexisNexis® True Cost of Fraud™ Study

North American Retail & Ecommerce

U.S. & Canada Edition

The LexisNexis® Risk Solutions True Cost of Fraud™ Study

Helping businesses navigate evolving fraud risks while fostering secure growth

The research provides a snapshot of:

- Current fraud trends in U.S. and Canadian ecommerce and retail markets
- Key pain points associated with digital transactions and emerging payment methods
- The evolving fraud landscape, including identity-based fraud, refund fraud and synthetic identity risks

Post-pandemic fraud landscape:

- Data collection for this report occurred during late 2024 and early 2025, reflecting fraud risks, challenges and costs influenced by post-pandemic consumer behavior shifts, increased digital transactions and fraudsters' adaptation to new fraud techniques.

This research covers consumer-facing fraud methods:

- Does not include insider fraud or employee fraud

The LexisNexis® Fraud Multiplier™ cost:

- Estimates the total cost impact of fraud beyond the direct transactional loss
- Factors in operational, legal and reputational expenses

Fraud Definitions:

- Fraudulent transactions due to identity fraud, which is the misuse of stolen payment 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

The study encompassed a broad survey of 569 risk and fraud executives in retail and ecommerce companies in the U.S. (487) and Canada (82).

Retailers and Ecommerce Merchants Include a Variety of Categories:

Segments

Segment Definitions:	Small Earns less than $10 million in annual revenues	Medium/Large Earns $10 million+ in annual revenues
# of Survey Completions	326	243

Call-Out Boxes Throughout Report:
S = Small retail/ecommerce
M/L = Medium/Large retail/ecommerce

Five Key Takeaways

1

Managing Customer Friction Is Critical to Fraud Prevention Success

Businesses must balance security, speed and ease of use, as excessive fraud prevention measures can lead to customer frustration and drop-off.

2

Fraud Continues to Escalate Across Channels, with Digital and Automated Threats on the Rise

Fraud continues to grow across various transaction channels, with online and mobile transactions being the most targeted.

3

Fraud's Financial and Operational Impact Extends Beyond Direct Losses

Fraud is not just about direct financial losses—it also strains operations, impacts customer retention and increases compliance burdens. Accounting for the full impact of fraud supports more comprehensive prevention approaches.

4

Identity Verification Gaps Undermine Fraud Prevention Efforts

Businesses face persistent challenges in identity verification during onboarding, while gaps in authentication and fraud detection effectiveness raise concerns about their ability to keep ahead of evolving threats.

5

A Variety of Fraud Prevention Solutions Exist, but Adoption Remains Limited, with an Overly Manual Approach

Businesses have access to multiple fraud mitigation strategies, including AI-driven models, behavioral biometrics and third-party fraud detection tools. Despite availability, adoption rates remain moderate, with many organizations still relying on outdated or incomplete approaches.

Recommendations

1

Balance Fraud Prevention with Customer Experience

Retailers need to strike a balance between fraud management effectiveness and customer experience. Passive risk assessment, based on behavioral biometrics or digital identity, can help to achieve this goal without active customer engagement.

2

Strengthen Identity Verification Across the Customer Journey

Confidence in identity helps to improve customer experience and also fraud capture. Enhance identity verification beyond physical attributes to include behavioral and digital identity intelligence at login and document authentication in higher-risk circumstances.

3

Enhance Automation While Maintaining Human Oversight

A strategic mix of AI-driven fraud detection and human oversight offers greater efficiency and scalability.

4

Invest in AI and Machine Learning for Scalable Fraud Detection

AI-powered solutions can detect anomalies and adapt to emerging fraud tactics in real time, enabling review teams to focus on more complex cases. Richer data insights into fraud analysis can break down data silos across divisions and organizations, enabling more efficient data sharing and anomaly detection.

5

Adopt a Multi-Layered Fraud Prevention Strategy

To better identify patterns and anomalies in customer behavior, use advanced data analytics powered by multiple forms of risk signals. This way, anti-fraud measures can better match the level of risk associated with each transaction or interaction, minimizing impact on low-risk legitimate customers.

KEY FINDING 1

Managing Customer Friction is Critical to Fraud Prevention Success

Impact of Fraud Prevention on Customer Churn: 62% of U.S. ecommerce businesses and 53% of Canadian ecommerce businesses report increased customer churn due to fraud prevention measures. 58% of U.S. retail businesses also experience heightened churn, highlighting the impact of security interventions on customer retention.

Fraud Prevention and Abandonment Factor: Primary drivers of abandonment, such as poor user experience (up to 37%), pricing confusion (up to 40%) and payment method restrictions or issues (up to 47%), demonstrate how fraud controls can unintentionally lead to customer drop-off.

Customer Trust as a Leading Priority: Improving customer trust and loyalty through seamless experiences ranks as the top fraud prevention priority for U.S. ecommerce (28%) and is a key focus across all segments. Minimizing fraud losses is a close second (peaking at 23% for Canada retail).

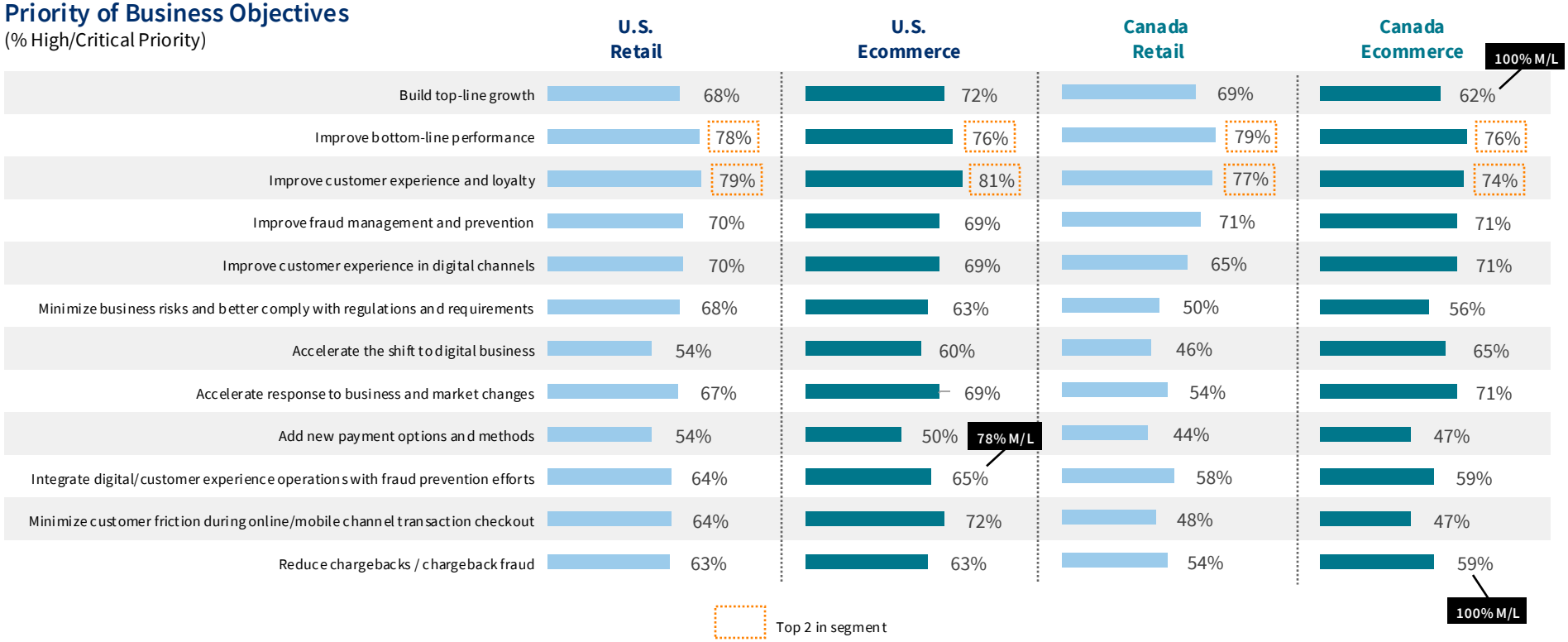
Balancing Growth and Fraud Prevention Is Critical for Business Objectives in 2025

Customer experience is a top priority. Improving customer experience and loyalty leads across all segments, with U.S. ecommerce and U.S. retail placing it as their highest priority. Canadian retail and ecommerce follow closely, emphasizing its importance for competitive advantage in an increasingly digital market.

Businesses must balance growth strategies with robust fraud prevention efforts, ensuring seamless customer experiences while protecting against evolving threats.

Priority of Business Objectives

(% High/Critical Priority)

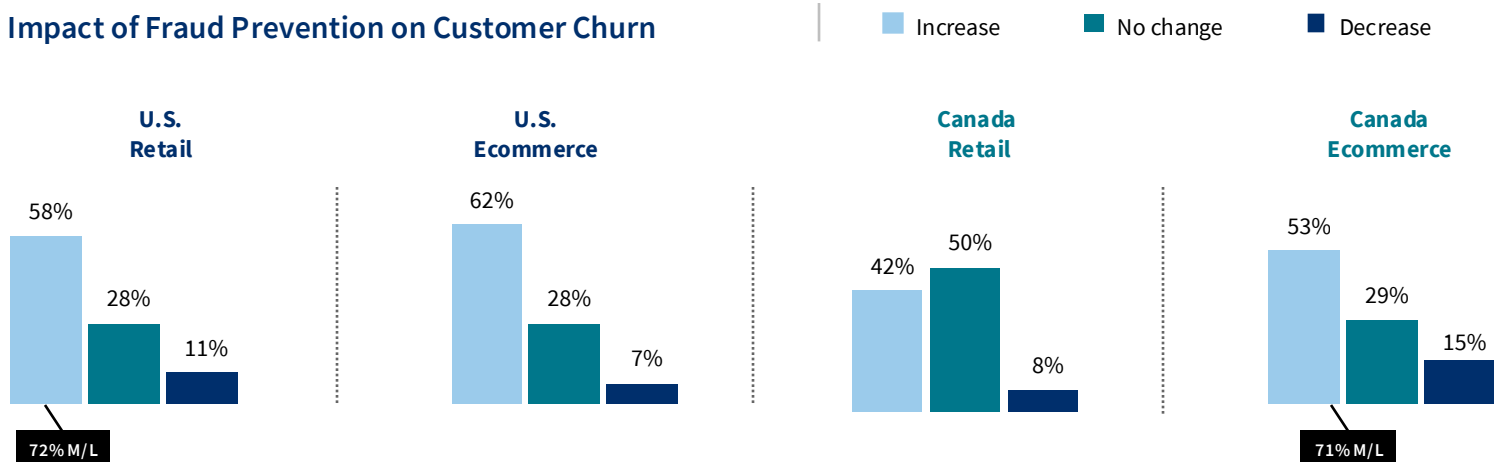


Question(s) 1

Fraud Prevention Measures Significantly Impact Customer Churn

62% of U.S. ecommerce and 53% of Canadian ecommerce report experiencing customer churn tied to fraud prevention measures, suggesting that digital-first businesses face greater sensitivity to friction in security processes.

58% of U.S. retail businesses report an increase in customer churn due to fraud prevention measures, indicating that security interventions may inadvertently deter legitimate customers if not optimized effectively.



Note: Percentages may not sum to 100% as the "Don't Know" responses are not shown.

Question(s) 4

User Experience and Payment Restrictions Drive Customer Abandonment

Across all customer journey stages, poor user experience, pricing confusion and payment restrictions are the primary drivers of abandonment. While security concerns play a role, friction in communication, checkout complexity and limited payment options contribute more significantly to drop-offs.

Primary Factors Contributing to Customer Abandonment During Key Journey Stages

(Top 2 per Segment)

	U.S. Retail	U.S. Ecommerce	Canada Retail	Canada Ecommerce
Account Creation / Onboarding	Poor user experience (36%)	Poor user experience (37%)	Lack of trust/security concerns (40%)	Lengthy or complicated processes (38%)
	Fraud-prevention friction (35%)	Lack of communication/response delays (35%)	Confusion over pricing, promotions or terms (33%)	Poor user experience (32%)
Cart Checkout	Confusion over pricing, promotions or terms (39%)	Confusion over pricing, promotions or terms (40%)	Confusion over pricing, promotions or terms (35%)	Lack of communication/response delays (41%)
	Poor user experience (35%)	Poor user experience (36%)	Fraud-prevention friction (35%)	Lengthy or complicated processes (38%)
Payment process	Payment method restrictions or issues (37%)	Payment method restrictions or issues (42%)	Payment method restrictions or issues (46%)	Payment method restrictions or issues (47%)
	Lack of trust/security concerns (35%)	Poor user experience (34%)	Confusion over pricing, promotions or terms (25%)	Lack of trust/security concerns (38%)

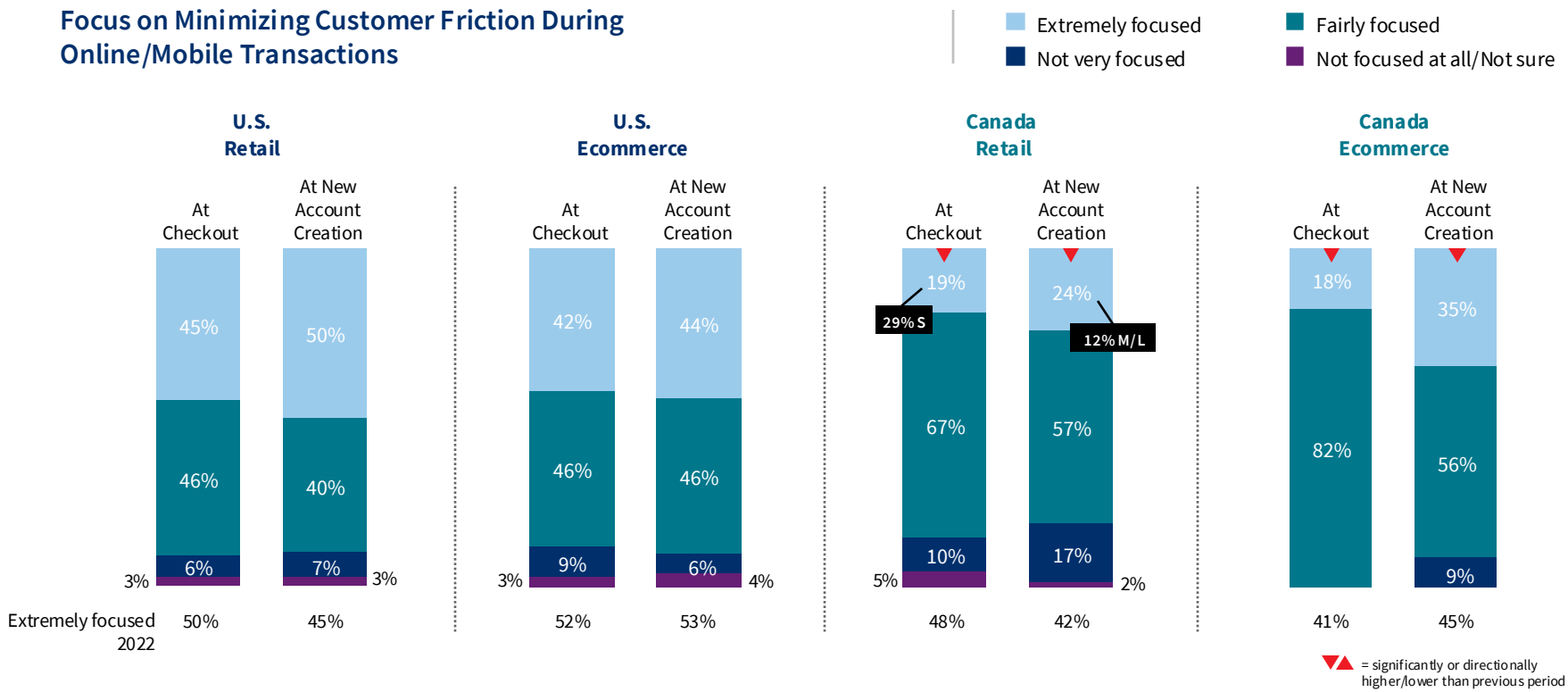
■ Question(s) 3C

Balancing Risk Mitigation with Customer Experience in Online Transactions

Businesses are increasingly focused on minimizing customer friction during checkout and new account creation, but regional differences in prioritization suggest varied risk tolerance and fraud mitigation strategies.

Businesses must ensure that fraud detection measures are aligned with user expectations, particularly in industries with high fraud exposure.

Focus on Minimizing Customer Friction During Online/Mobile Transactions



Question(s) 34 & 35A

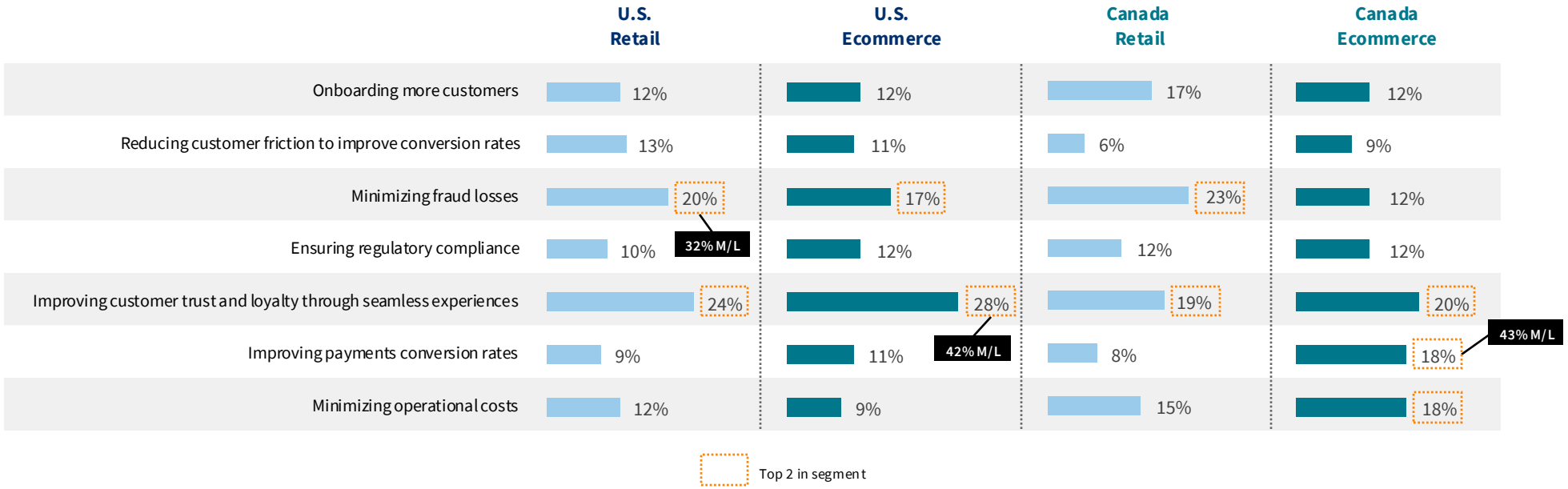
Strengthening Customer Trust as a Leading Fraud Prevention Priority

Organizations are increasingly prioritizing customer trust and loyalty, recognizing that seamless experiences are key to long-term retention. Fraud prevention efforts are evolving to balance security with customer satisfaction.

Minimizing fraud losses ranks as the second-highest priority across multiple segments, particularly in Canadian retail. Businesses continue to refine their fraud mitigation efforts while maintaining customer confidence.

Organization's Priorities for Fraud Prevention and Customer Experience

(ranked 1st)



Question(s) 2

KEY FINDING 2

Fraud Continues to Escalate Across Channels, with Digital and Automated Threats on the Rise

Synthetic Identity Fraud Is a Growing Concern: Fraudsters exploit synthetic identities—blending real and fake information—to bypass traditional verification methods. This is especially prevalent in new account creation, where U.S. businesses report synthetic identity fraud accounts for around 30% of fraud losses across the customer journey. Canadian businesses also see high levels.

Purchase Transactions Are the Primary Target for Fraud: Fraudsters commit identity-related fraud across various stages of the customer journey, with purchase transactions representing the highest concentration due to high transaction volumes and payment vulnerabilities. In this stage, identity-related fraud accounts for 45% of cases in U.S. ecommerce and 42% in Canadian retail. Identity-related fraud during account creation remains significant, ranging from 29% in U.S. ecommerce to 32% in Canadian ecommerce.

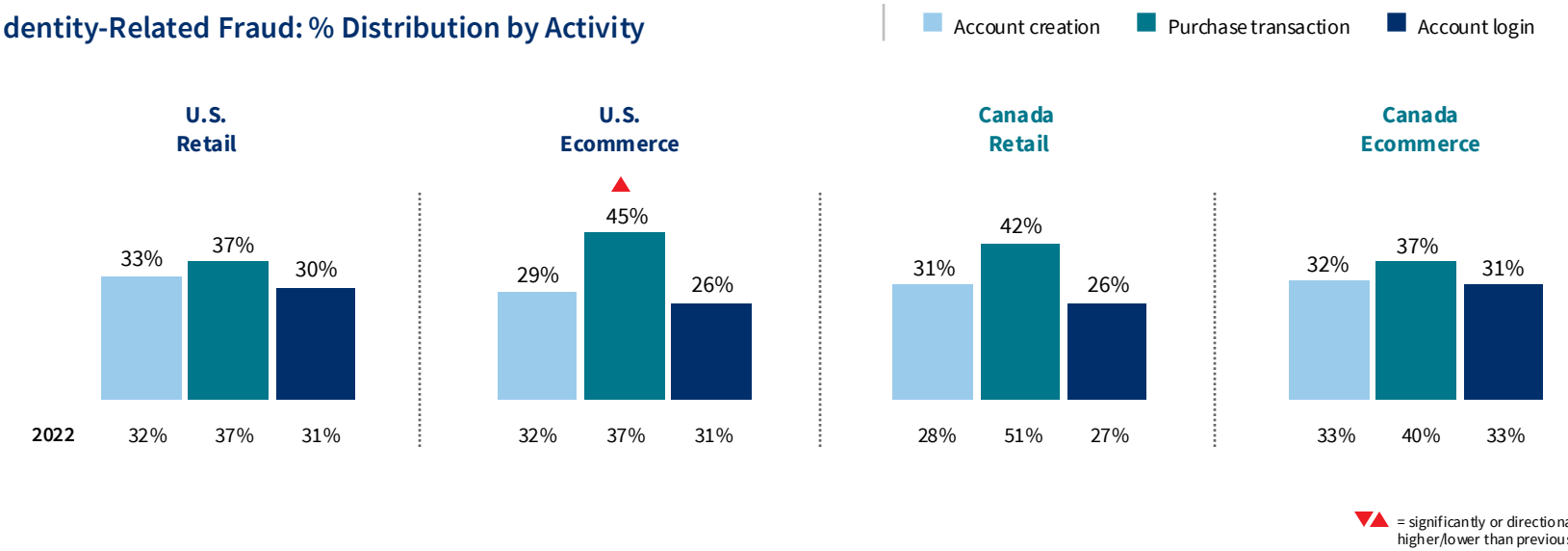
Automated Fraud Tactics Are Evolving: Malicious bot activity remains a persistent threat, with over one-third of businesses reporting an increase in bot attacks over the past year. While bots may represent a smaller share of total fraud, their intensity and frequency are rising, indicating evolving fraud strategies.

Identity-Related Fraud Predominantly Targets Purchase Transactions but Impacts All Customer Journey Stages

Across all segments, purchase transactions account for the highest proportion of identity-related fraud, peaking at 42% in Canadian retail and 45% in U.S. ecommerce. The high volume of transactions in this phase presents fraudsters with numerous opportunities to exploit.

Fraud during account creation remains significant, ranging from 29% in U.S. ecommerce to 32% in Canadian ecommerce. Fraudsters leverage stolen or synthetic identities during this phase to set the foundation for future fraudulent activities.[1]

Identity-Related Fraud: % Distribution by Activity



Question(s) 11B

1: https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud

Fraud Losses Vary by Type Across Customer Journey Phases, Highlighting Diverse Threats

Synthetic Identity Fraud Is a Growing Concern: Fraudsters continue to exploit synthetic identities—blending real and fake information—to bypass traditional verification methods. This type of fraud is particularly prevalent in new account creation, where businesses struggle to differentiate real customers from fraudulent ones.

Businesses cite synthetic identity fraud as one of the hardest types to detect and mitigate, particularly in ecommerce. Without real-time identity verification and behavioral analysis, fraudsters can continue to establish accounts and transact undetected, driving financial and operational risks.

% Distribution of Fraud Losses by Fraud Type

U.S. Retail

	Friendly/ 1st Party Fraud	3rd Party/ Synthetic Identity Fraud	3rd Party Account Takeover	Lost/Stolen Merchandise	Fraudulent Request for Return
New Account Creation	29%	31%	11%	14%	15%
2022	29%	30%	14%	14%	13%
Purchase Transactions	28%	28%	10%	19%	15%
2022	26%	26%	14%	19%	15%
Account Login	29%	29%	13%	14%	14%
2022	27%	27%	14%	17%	15%

U.S. Ecommerce

	Friendly/ 1st Party Fraud	3rd Party/ Synthetic Identity Fraud	3rd Party Account Takeover	Lost/Stolen Merchandise	Fraudulent Request for Return
New Account Creation	28%	31%	11%	14%	17%
2022	31%	28%	14%	13%	14%
Purchase Transactions	29%	29%	10%	14%	18%
2022	30%	28%	13%	13%	16%
Account Login	27%	33%	11%	12%	17%
2022	31%	29%	13%	12%	15%

Question(s) 11A

Synthetic Identity Fraud and Account Takeover Are Growing Threats in Canadian Retail and Ecommerce

Synthetic Identity Fraud Remains a Leading Threat: Canadian retail and ecommerce continue to see high levels of synthetic identity fraud, particularly in purchase transactions. Fraudsters are leveraging synthetic identities to make fraudulent purchases and manipulate return policies, posing a major challenge for businesses.

With fraudsters using synthetic identities to create seemingly legitimate accounts, account takeover is becoming more sophisticated. Once an account is established, bad actors can exploit it for various fraud schemes, including unauthorized purchases and financial crimes.

% Distribution of Fraud Losses by Fraud Type

Canada Retail

	Friendly/ 1st Party Fraud	3rd Party/ Synthetic Identity Fraud	3rd Party Account Takeover	Lost/Stolen Merchandise	Fraudulent Request for Return
New Account Creation	26%	27%	18%	15%	14%
2022	29%	31%	14%	12%	14%
Purchase Transactions	28%	24%	13%	20%	15%
2022	23%	21%	14%	25%	17%
Account Login	25%	25%	22%	16%	12%
2022	24%	26%	14%	17%	19%

Canada Ecommerce

	Friendly/ 1st Party Fraud	3rd Party/ Synthetic Identity Fraud	3rd Party Account Takeover	Lost/Stolen Merchandise	Fraudulent Request for Return
New Account Creation	32%	30%	12%	10%	16%
2022	30%	31%	13%	13%	13%
Purchase Transactions	31%	35%	9%	13%	12%
2022	26%	35%	11%	11%	17%
Account Login	29%	28%	18%	9%	16%
2022	27%	32%	14%	12%	15%

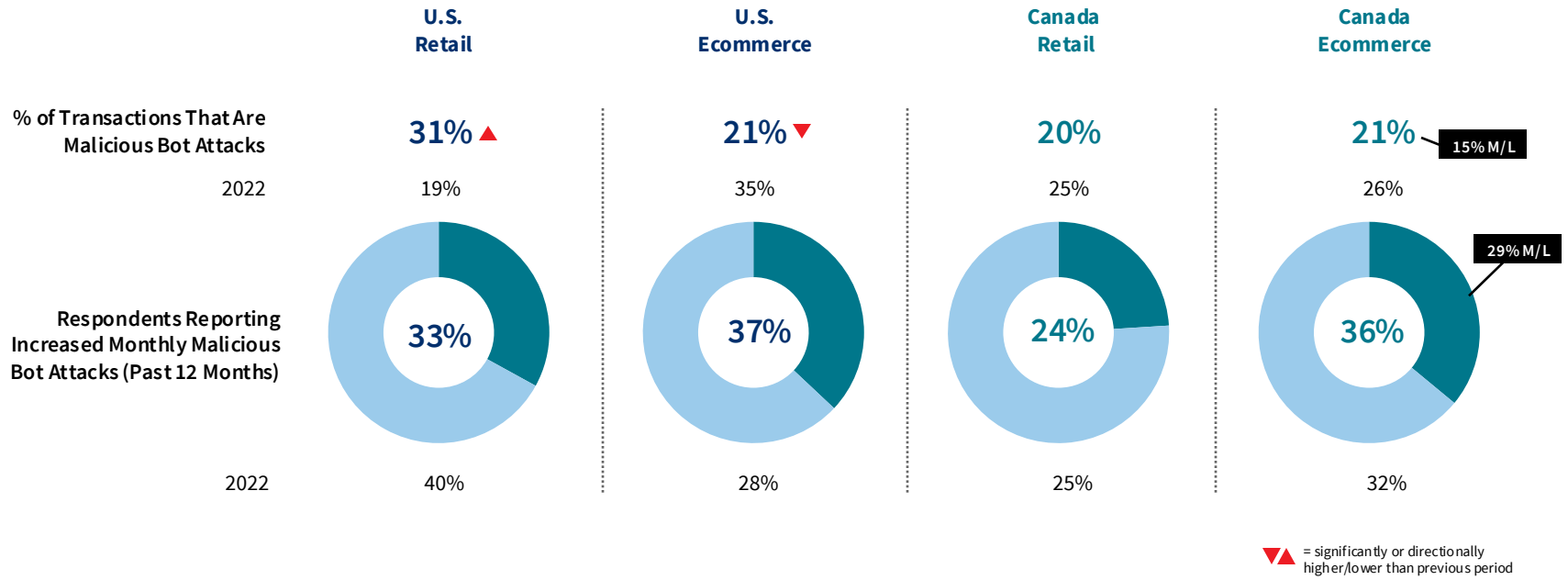
Question(s) 11A

Evolving Dynamics in Malicious Bot Attacks Reflect Shifting Threat Patterns

The percentage of transactions attributed to malicious bot attacks has decreased in some markets, such as U.S. ecommerce. However, over one-third of respondents in this segment report an increase in bot attacks over the past 12 months. Bots may now represent a smaller share of total transactions, but the intensity and frequency of attacks are escalating, reflecting a shift in fraudsters' strategies.

The heightened focus on U.S. and Canadian ecommerce channels aligns with global fraud trends, in which digital-first commerce remains a primary target. As fraudsters adapt to businesses' defenses, malicious bot activity persists as a top challenge despite reductions in some metrics.[2]

Malicious Bot Attacks



■ Question(s) 29A & 29B

2: https://risk.lexisnexis.com/global/en/insights-resources/article/detect-and-mitigate-bot-attacks

KEY FINDING 3

The Financial and Operational Impact of Fraud Extends Beyond Direct Losses

The Toll of Fraud Is Rising: The LexisNexis® Fraud Multiplier™ cost continues to increase ($4.61 for U.S. and $4.52 for Canada), indicating that every dollar lost to fraud carries escalating financial and operational consequences.

Fraud Costs Remain Widely Distributed Across Payment Methods: Mobile transactions (including digital wallets, peer-to-peer payments and QR codes) contributing a notable share (41% in Canada ecommerce, 35% in U.S. ecommerce).

Digital Transactions Drive the Highest Fraud Costs: Online and mobile transactions make up the largest share of fraud losses, with U.S. ecommerce seeing 30% of fraud costs coming from mobile channels and 53% from online purchases. Canadian ecommerce is also heavily impacted, with 37% of fraud costs linked to mobile transactions.

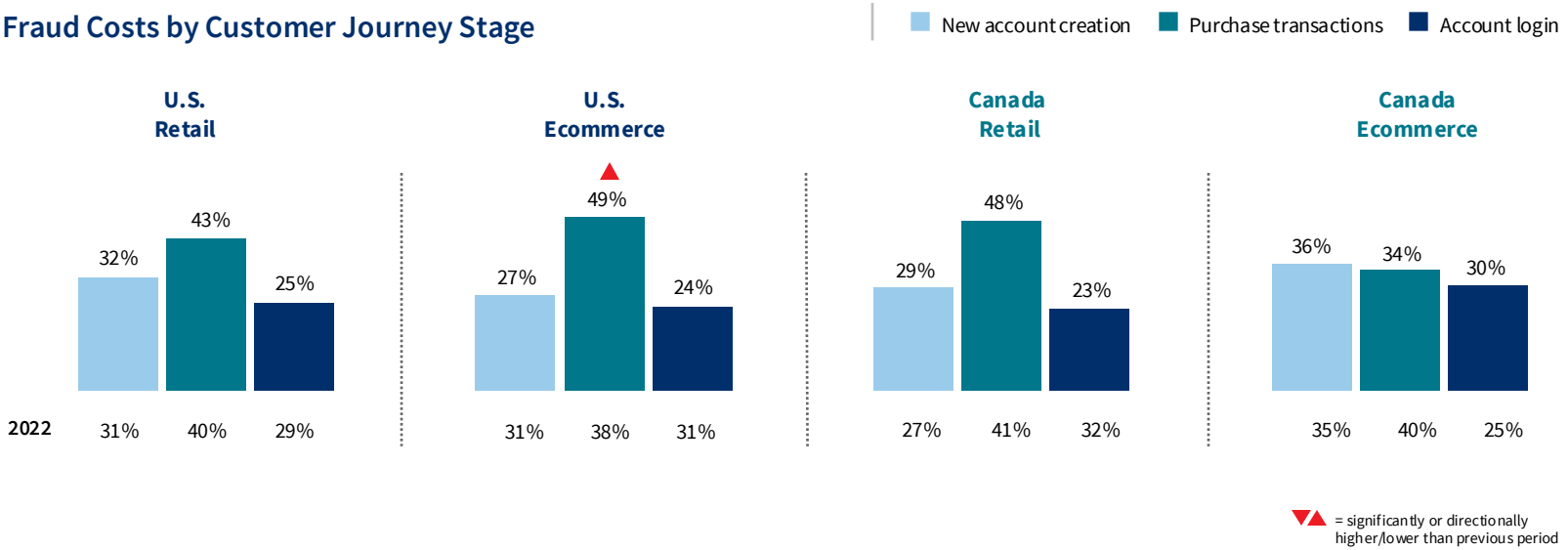
Customer Trust Takes a Hit: Fraud contributes to customer churn and increases the resource commitment required for fraud management (up to 81% indicate). Nearly two-thirds of businesses report moderate to significant impacts across multiple areas, highlighting the challenge of balancing security with a seamless customer experience.

Fraud Costs Concentrated in Purchase Transactions, but Risks Span All Customer Journey Stages

In both U.S. and Canadian markets, purchase transactions account for the largest share of fraud costs, with U.S. ecommerce reporting the highest percentage at 49%. The complexity and volume of transactions during this phase make it a lucrative target for fraudsters.

Fraud costs from account creation remain substantial, particularly in Canadian ecommerce (36%). Fraudsters exploit weaknesses in onboarding processes to create fake accounts or use stolen identities, leading to downstream fraud risks.

% Fraud Costs by Customer Journey Stage



Question(s) 10B

The LexisNexis Fraud Multiplier™ Cost Increases

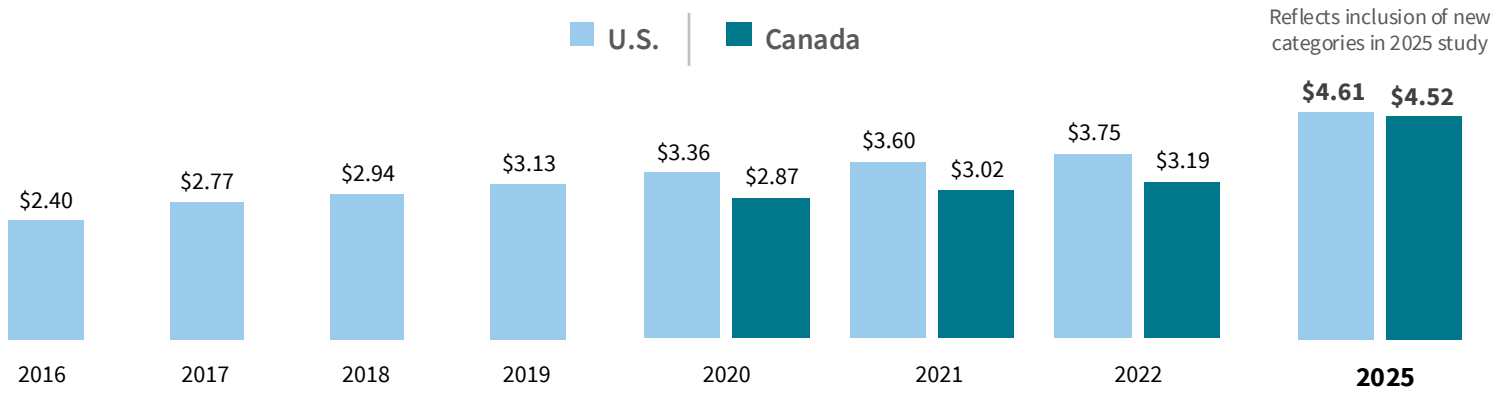
Significant Cost Growth: Every dollar lost to fraud costs U.S. merchants **$4.61** and Canadian merchants **$4.52**. This shows that fraud's impact goes beyond direct financial losses, encompassing operational, reputational and compliance costs.

Since 2016, the cost has steadily increased, underscoring the growing complexity and expense of combating fraud.

Organizations must consider the comprehensive costs of fraud when assessing risk mitigation strategies. Investing in advanced fraud detection and prevention tools, such as AI-driven solutions and real-time monitoring, is critical to reducing the toll of fraud on businesses.[3]

Canada's fraud multiplier grew more due to a mix of advanced credit card usage, weaker verification systems and stronger consumer protection policies that fraudsters exploit.

Cost of Fraud: LexisNexis Fraud Multiplier™



Question(s) S9, 10A, 15A

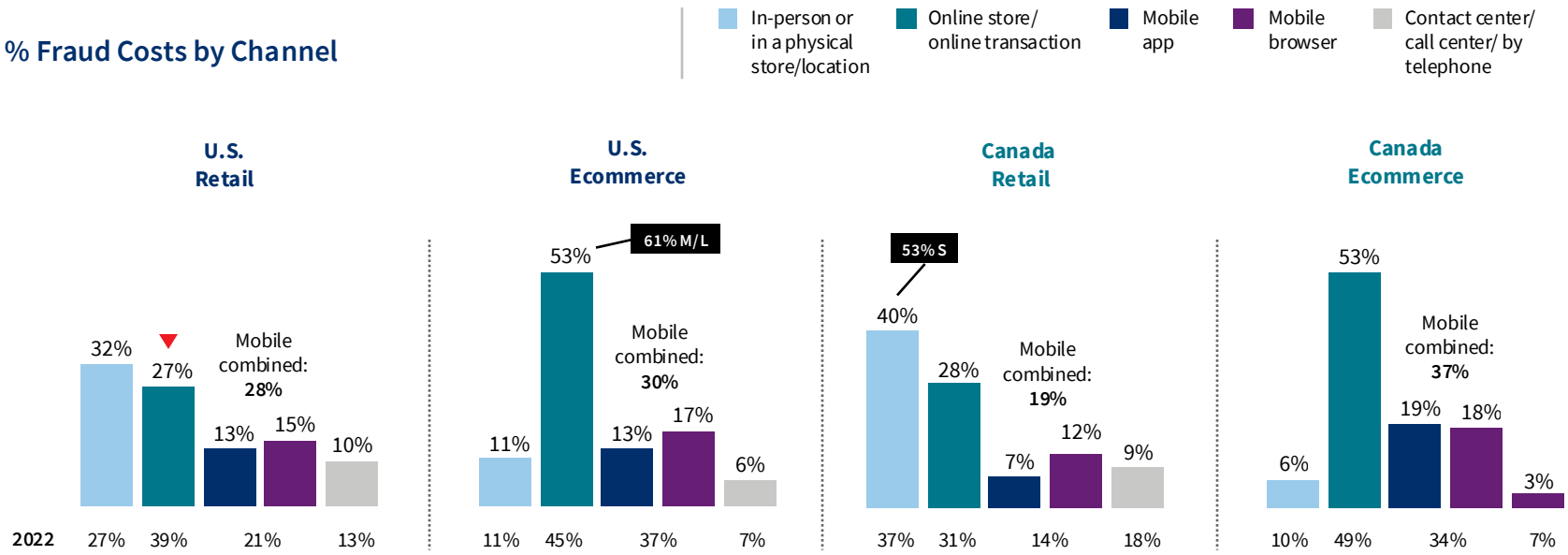
3: Singh, N., & Sharma, P. (2023). A comprehensive review on fraud detection techniques and trends in financial services. International Journal of System Assurance Engineering and Management. Springer.

Fraud Costs Vary by Channel, Highlighting the Disproportionate Impact of Online and Mobile Transactions

In both U.S. and Canadian ecommerce, online transactions account for the largest share of fraud costs, with more than half of the burden in these markets. This underscores the critical need to strengthen security measures in online payment environments.

Mobile transactions contribute significantly to fraud costs, with U.S. ecommerce seeing a combined 30% share and Canadian ecommerce reporting 37%.

% Fraud Costs by Channel



Note: Percentages may not sum to 100% as the "Other" responses are not shown.

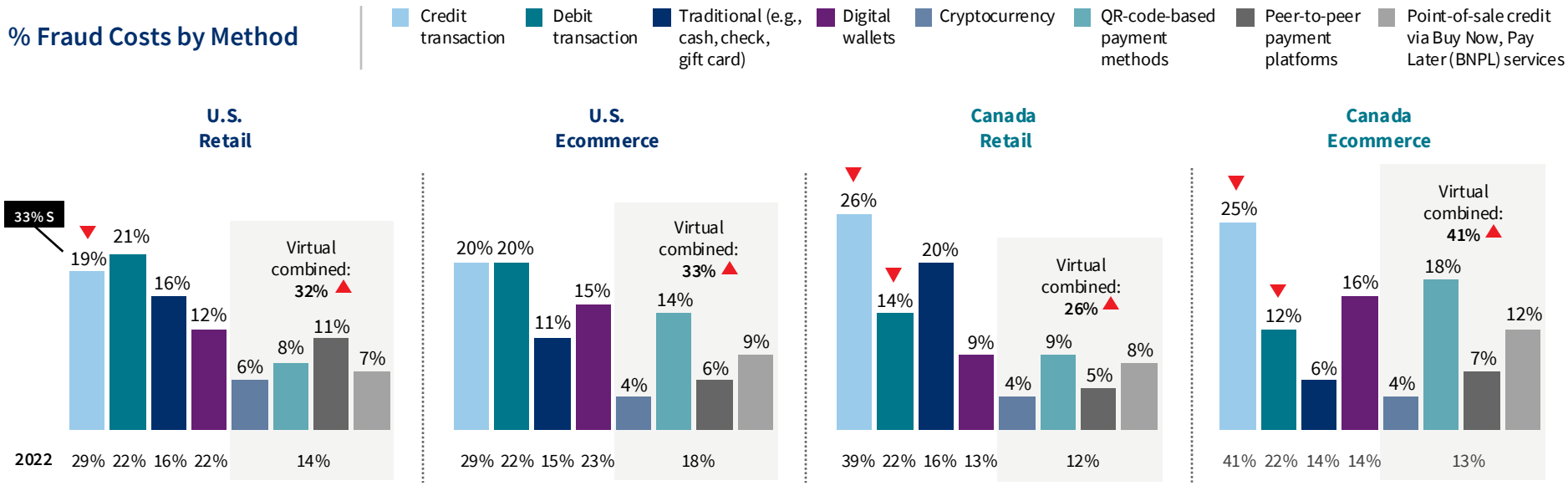
▼▲ = significantly or directionally higher/lower than previous period

Question(s) 14

Fraud costs remain widely distributed across payment methods, with mobile transactions (including digital wallets, peer-to-peer payments and QR codes) contributing a notable share.

Mobile payments continue to be a rising fraud target, reinforcing the need for stronger authentication and fraud detection tools specifically tailored for mobile transactions.

% Fraud Costs by Method



Note: Percentages may not sum to 100% as the "Other" responses are not shown.

▼▲ = significantly or directionally higher/lower than previous period

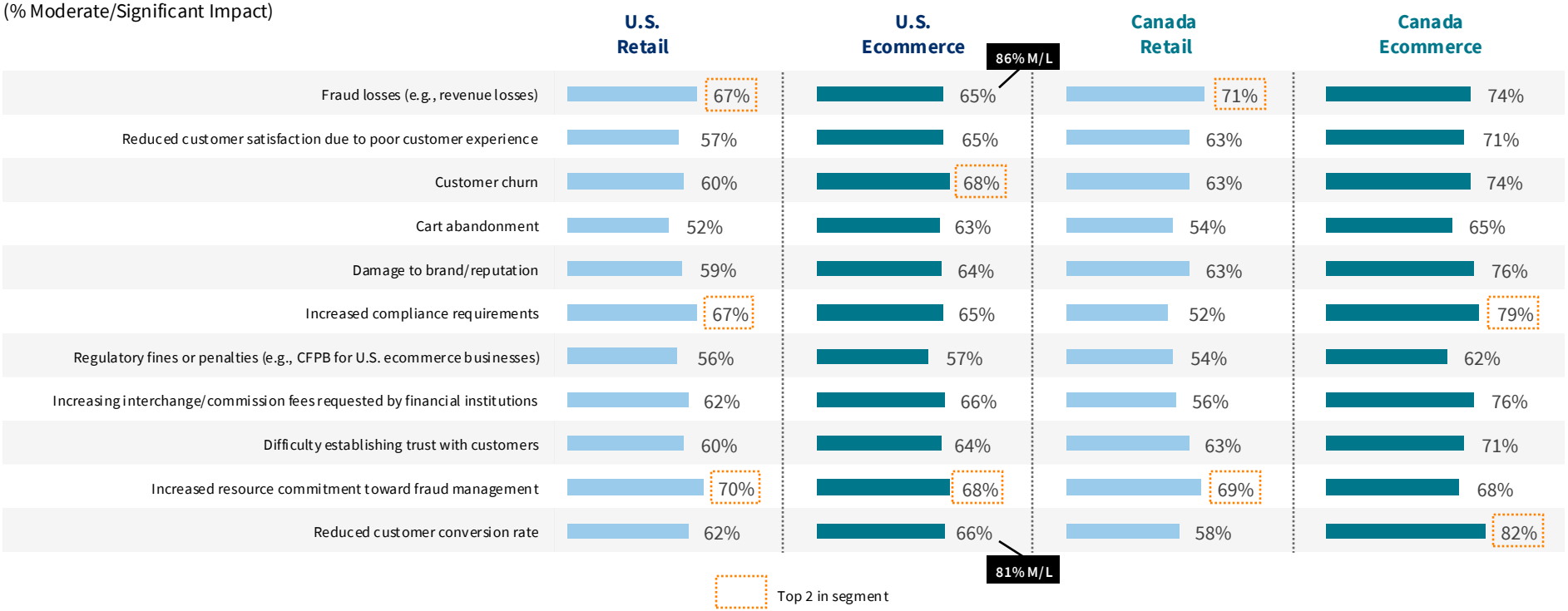
Question(s) 17

Fraud Significantly Impacts Revenue, Customer Trust and Operational Efficiency Across Regions

Fraud not only impacts revenue but also erodes customer trust, loyalty and brand integrity. Of note, fraud has an especially significant impact on increasing fees for U.S. ecommerce (35%) and on cart abandonment for Canadian ecommerce (35%). Businesses must invest in advanced fraud prevention tools that protect against immediate threats while minimizing customer friction to sustain both operational efficiency and competitive advantage.

Impact of Fraud on Business Areas

(% Moderate/Significant Impact)



Question(s) 3

KEY FINDING 4

Identity Verification Gaps Undermine Fraud Prevention Efforts

Identity Fraud Is a Persistent Threat During Account Creation: Fraudsters exploit vulnerabilities in onboarding, with identity verification ranking among the top challenges across all segments—up to 48% of businesses cite it as a significant issue.

Email or Device Verification Also Ranked Highly: As many as 41% of businesses ranking it as a top 3 challenge.

Confidence in Fraud Detection May Be Misleading: While over 70% of businesses rate their fraud detection as "mostly effective" or better, gaps in verification and authentication raise questions about their ability to combat evolving fraud tactics.

Optimism in Future Fraud Detection May Overlook Key Risks: For instance, 79% of U.S. ecommerce businesses expect fraud detection to improve, yet persistent vulnerabilities in identity verification could leave them exposed.

Identity Verification Remains the Biggest Challenge Across Fraud Touchpoints

Verification of customer identity ranks among the top fraud challenges for all key stages—new account creation, purchase transactions and account login. The need for email/device verification and phone verification also highlights the growing complexity of authenticating legitimate users while preventing fraud.

Top Three Ranked ONLINE and MOBILE Fraud Challenges | United States

		New Account Creation		Purchase Transactions		Account Login	
		Retail	Ecommerce	Retail	Ecommerce	Retail	Ecommerce
Identity	Document authentication	25%	22%	24%	22%	22%	20%
	Email or device verification	26%	33%	22%	24%	31%	40%
	Verification of customer identity	41%	37%	36%	30%	37%	32%
	Phone verification	25% 49% S	22%	27%	32%	31%	30%
Transaction	Address verification	21%	29%	23%	30%	22%	28%
	Multiple entity relationship analysis	22%	22%	21%	29% 39% M/L	26%	19%
	Determining transaction source	21%	24%	20%	24%	17%	18%
	Lack international fraud tools	22%	18%	21%	17%	19%	27%
	New transaction methods	18%	17%	22%	15%	20%	15%
Impacts	Identifying malicious bots	21%	27%	25%	22%	18%	23%
	Assessing fraud risk by country	16%	13%	16%	14%	18%	18%
	Excessive manual order reviews	15%	15%	19%	17%	18%	10%
	Balance fraud prevention with the customer experience	26%	21%	24%	24%	21%	20%

Top 2 in segment

Question(s) 20

Identity Verification Also Remains a Top Fraud Challenge in Canada

Verification of customer identity ranks as the leading fraud challenge across all major touchpoints—new account creation, purchase transactions and account login. Email and device verification also emerge as critical concerns, particularly in Canadian ecommerce.

Top Three Ranked ONLINE and MOBILE Fraud Challenges | Canada

		New Account Creation		Purchase Transactions		Account Login	
		Retail	Ecommerce	Retail	Ecommerce	Retail	Ecommerce
Identity	Document authentication	**21%**	**18%**	**21%**	**12%**	**17%**	**9%**
	Email or device verification	26%	41%	29%	32%	36%	35%
	Verification of customer identity	38%	32%	38%	44%	48%	32%
	Phone verification	29%	26%	29%	26%	26%	24%
	Address verification	24%	24%	19%	21%	21%	21%
Transaction	Multiple entity relationship analysis	31%	24%	33%	12%	17%	18% 43% M/L
	Determining transaction source	21%	24%	31%	12%	19%	21%
	Lack international fraud tools	24%	21%	14%	18%	17%	26%
	New transaction methods	21%	18%	14%	21% 57% M/L	31%	21%
Impacts	Identifying malicious bots	17%	15%	19%	32%	17%	24%
	Assessing fraud risk by country	14%	15%	12%	32%	17%	18%
	Excessive manual order reviews	10%	18%	12%	26% 43% M/L	10%	26%
	Balance fraud prevention with the customer experience	24%	26% 43% M/L	29%	12%	26%	26% 43% M/L

Top 2 in segment

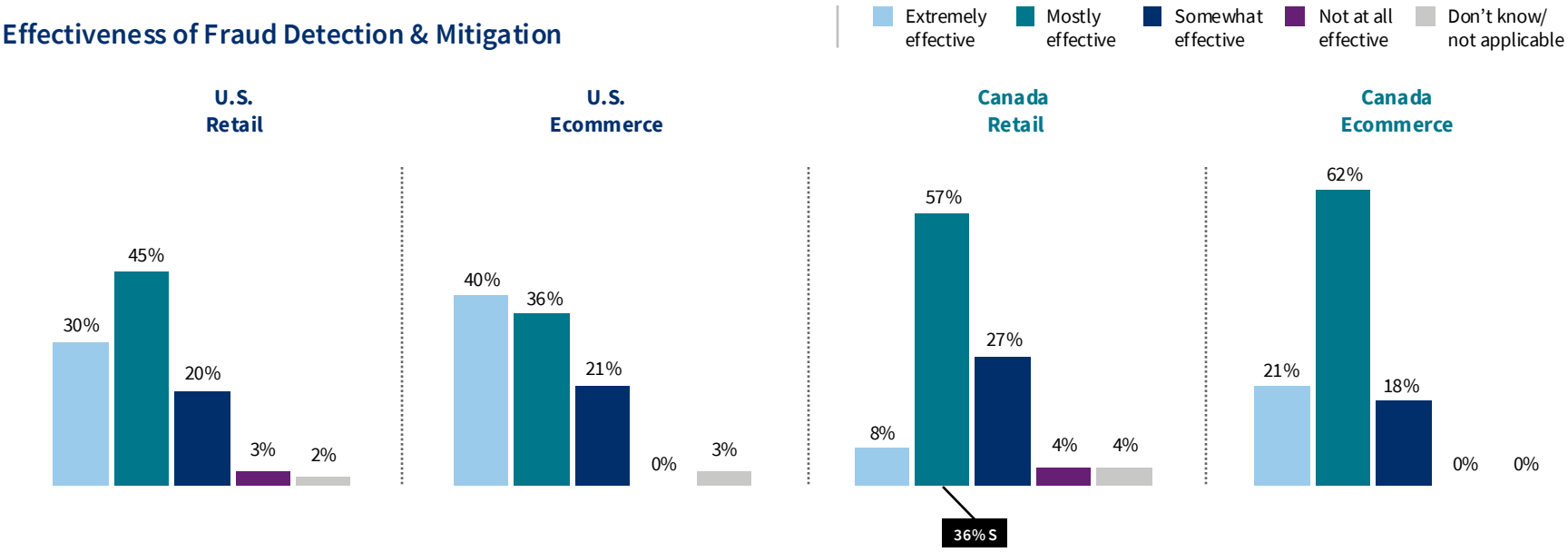
Question(s) 20

Confidence in Fraud Detection May Be Misleading

While many businesses rate their fraud detection as “effective,” this confidence may be overstated. Some organizations may not fully recognize the extent of fraud they face, while others hesitate to acknowledge vulnerabilities or implement stricter controls that could introduce customer friction.

Organizations may be prioritizing frictionless transactions over rigorous fraud detection, potentially leaving gaps in fraud prevention strategies.

Effectiveness of Fraud Detection & Mitigation



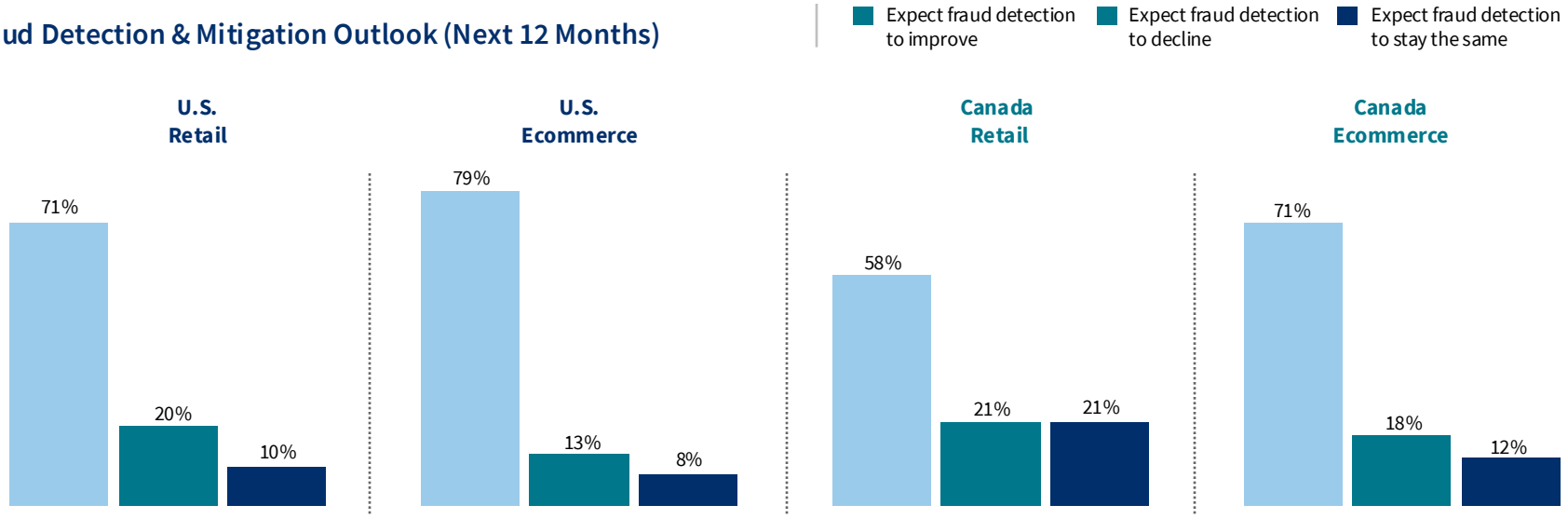
Question(s) 42

Confidence in Future Fraud Detection May Be Overly Optimistic

Most businesses, particularly in U.S. retail and ecommerce, anticipate improvements in their fraud detection capabilities. However, this optimism may not fully account for evolving fraud tactics, emerging threats or gaps in fraud mitigation strategies. Canadian retail, with a more cautious outlook, may reflect a more realistic assessment of ongoing fraud challenges.

Businesses projecting improved fraud detection may underestimate the sophistication of new fraud tactics, potentially leaving them exposed.

Fraud Detection & Mitigation Outlook (Next 12 Months)

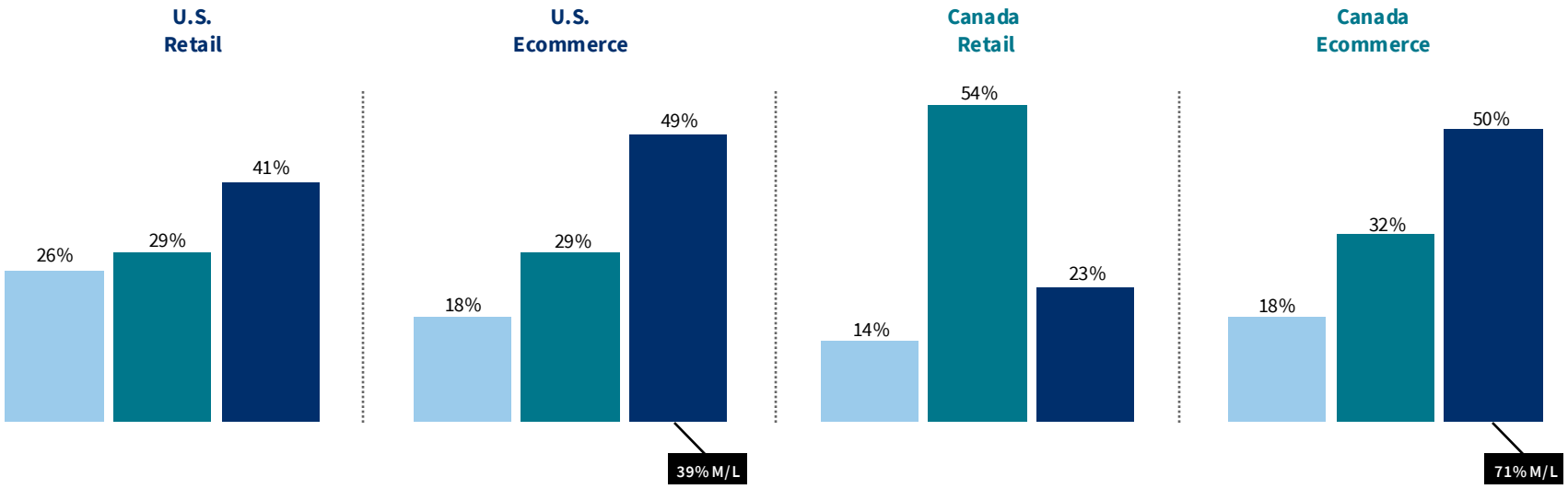


Question(s) 43

While many businesses plan to maintain or slightly increase fraud prevention budgets, notable differences exist between Canadian and U.S. markets, as well as between retail and ecommerce.

Many businesses across all segments expect their fraud prevention budgets to stay the same. This suggests that organizations feel their current fraud strategies are sufficient but remain cautious about significant new investments. In U.S. ecommerce, almost half of businesses plan to increase budgets slightly (+6% to +10%), indicating a steady commitment to fraud prevention as digital transactions continue to grow. Canadian ecommerce follows a similar pattern.

Anticipated Changes in Fraud Prevention Budget



Question(s) 44

KEY FINDING 5

A Variety of Fraud Prevention Solutions Exist, but Adoption Remains Limited, with an Overly Manual Approach

Machine Learning Is Gaining Traction, but Adoption Varies: While machine learning is increasingly used for fraud prevention, its application differs by region and sector. Canadian ecommerce leads in ML adoption for fraud prevention, with 53%-71% usage across key fraud types, compared to 56%-68% in U.S. ecommerce.

Limited Use of Shared Intelligence Leaves Businesses Vulnerable: Merchants are underutilizing third-party risk intelligence consortiums, with as little as 3%-6% adoption in some segments. Without these collaborative platforms, businesses are left to combat fraud in isolation, increasing risks and negatively impacting customer experience.

Authentication Gaps Undermine Fraud Prevention Strategies: Retailers rely on government-issued IDs at checkout but disagree on the importance of document authentication capabilities, signaling an opportunity in fraud prevention strategies.

Over 40% of Businesses Still Rely Heavily on Manual Fraud Prevention: Around two-thirds of organizations continue to use a mix of manual and automated processes, with only a small portion (around 4%) fully adopting automation.

Expanding Role of Machine Learning in Fraud Prevention

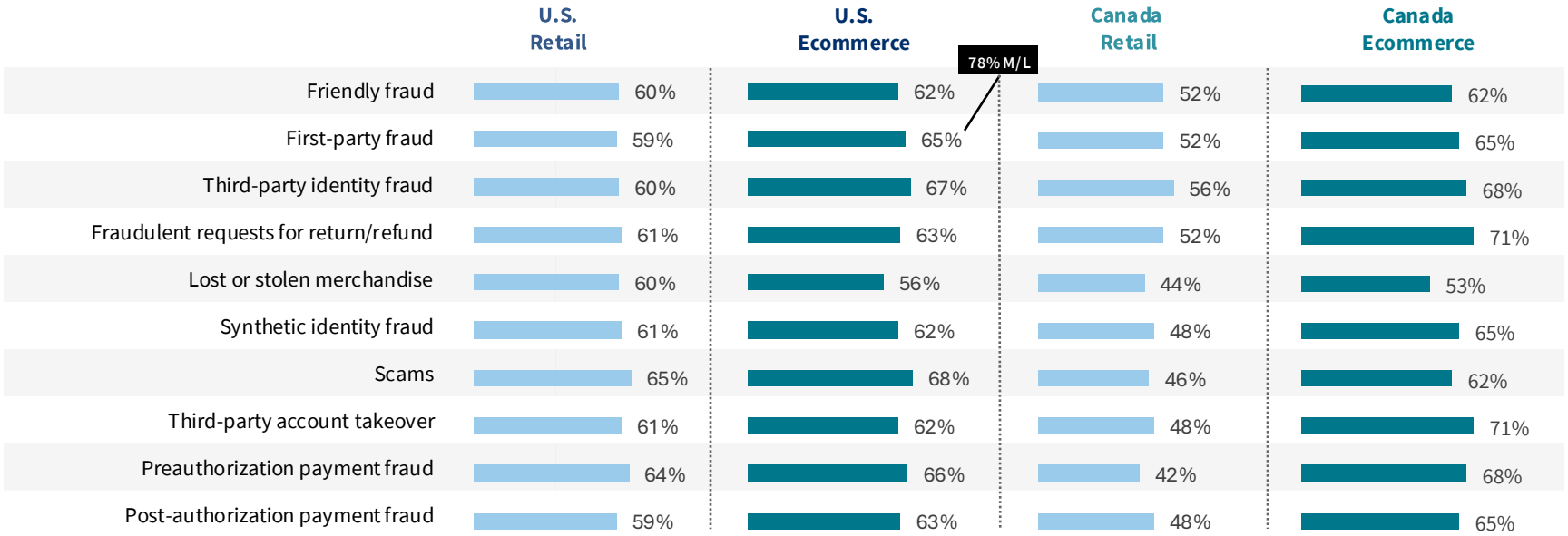
Businesses are leveraging machine learning (ML) to combat diverse fraud types, with notable adoption across various fraud categories. Machine learning is widely used across fraud categories, with particularly high adoption in preauthorization payment fraud, scams and third-party fraud.

U.S. and Canada show differing priorities, with Canadian retail demonstrating comparatively lower ML adoption in some fraud areas. Ecommerce segments in both countries maintain a stronger reliance on ML to address synthetic and identity-based fraud risks.

Ecommerce sectors, particularly in Canada, are leveraging ML more aggressively to combat synthetic identity fraud, recognizing its role in addressing large-scale, automated fraud attacks.

Use of Machine Learning for Fraud Prevention

(% Commonly Used / Primary Tool)



Question(s) 32

Fraud Prevention Strategies Differ by Channel, Highlighting Gaps in Advanced Authentication in the U.S.

Fraud prevention approaches are fragmented across the customer journey. Businesses apply different fraud mitigation solutions depending on the transaction point, but gaps exist in integrating a seamless, layered security strategy across account creation, cart checkout and payment process.

Use of the Following Fraud Mitigation Solutions

(Top 3 per Segment)

	U.S. Retail	U.S. Ecommerce
Account Creation / Onboarding	Email & Risk Verification	Email & Risk Verification
	Check Verification	Phone # Risk Verification
	Name/Address/DOB Verification	Geolocation
Cart Checkout	Authenticate Using Payment Instrument	Authenticate Using Payment Instrument
	Authenticate Using Behavioral Metrics	OTP/2 Factor
	Gov't-Issued ID	Geolocation
Payment process	OTP/2 Factor	Email & Risk Verification
	Authenticate Using Biometrics	OTP/2 Factor
	Device ID	Phone # Risk Verification

Fraud solutions should do more than prevent risk—they should enhance **customer experience.** Seamless authentication, like biometrics and geolocation, reduces friction while maintaining security, strengthening trust and loyalty.

Question(s) 30

Fraud Prevention Approaches in Canada Reflect a Mix of Traditional and Advanced Methods

Fraud prevention approaches are fragmented across the customer journey. Businesses apply different fraud mitigation solutions depending on the transaction point, but gaps exist in integrating a seamless, layered security strategy across account creation, cart checkout and payment process.

Use of the Following Fraud Mitigation Solutions

(Top 3 per Segment)

	Canada Retail	Canada Ecommerce
Account Creation / Onboarding	Check Verification	OTP/2 Factor
	Email & Risk Verification	Email & Risk Verification
	OTP/2 Factor	Phone # Risk Verification
Cart Checkout	Gov't-Issued ID	Geolocation
	Authenticate Using Payment Instrument	Automated Transaction scoring
	Real-time Fraud	Check Verification
Payment process	Email & Risk Verification	Email & Risk Verification
	Quiz or KBA	Check Verification
	Device ID	Name/Address/DOB Verification

Fraud solutions should do more than prevent risk—they should enhance **customer experience.** Seamless authentication, like biometrics and geolocation, reduces friction while maintaining security, strengthening trust and loyalty.

Question(s) 30

Fraud Management Priorities Highlight Demand for Service-Driven Solutions

Fraud-management administrator management is a top priority in U.S. retail, U.S. ecommerce and Canadian retail, highlighting the need for centralized fraud oversight. Card-payment and mobile/online-payment fraud models are also key features, especially in Canadian ecommerce and U.S. retail, as businesses strengthen payment fraud detection amid growing digital transactions.

These key features should be understood within the broader context of balancing fraud prevention with a seamless customer experience. Effective fraud management isn't just about stopping fraud—it's about integrating security measures that protect businesses while ensuring smooth, hassle-free interactions for legitimate customers.

Key Features of an Effective Fraud Management Solution

(Ranked in Top 3)

	U.S. Retail	U.S. Ecommerce	Canada Retail	Canada Ecommerce
Consortium, third-party data integration	13%	6%	4%	3%
Rules-based risk scoring and alerting	14%	14%	13%	12%
Account-takeover detection	19%	13%	17%	24%
Link analysis	9%	12%	15%	21%
AI and ML models usage	19%	22%	23%	41%
Ease of rule management/self-serve modelling	16%	24%	25%	24%
Model explainability and governance	9%	9%	8%	21%
Card-payment fraud models	26%	20%	29%	32%
Mobile/online-payment fraud models	27%	24%	15%	24%
Fraud-management-administrator management*	34%	39%	42%	21%
Global network intelligence	19%	24%	23%	21%
Reporting and dashboarding	14%	12%	19%	6%
Case management	14%	11%	13%	15%
Device intelligence	18%	21%	6%	9%
Segmentation and behavioral profiles of customers and attributes	14%	13%	15%	15%
Document authentication	20%	23%	23%	12%
Behavioral biometrics	15%	14%	13%	3%

71% M/L

53% M/L

Question(s) 31

Top 2 in segment

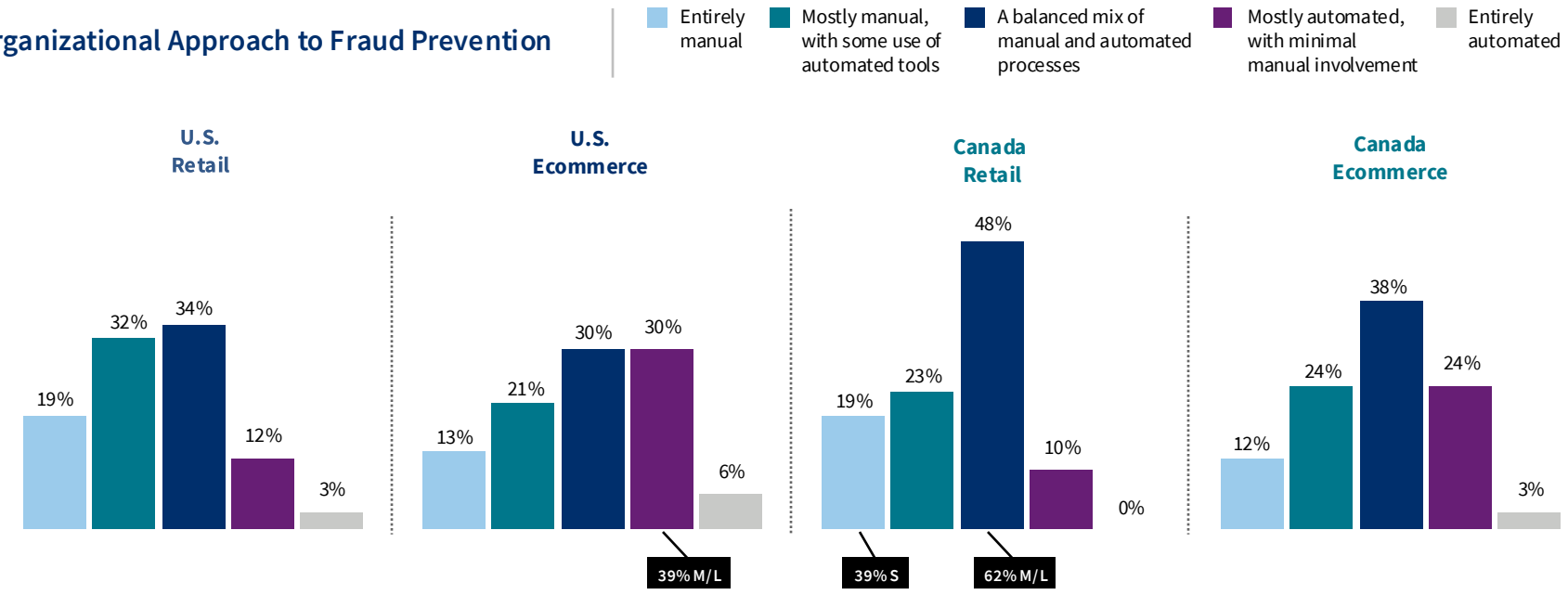
***Fraud-management-administrator management** refers to overseeing fraud prevention tools, policies and operations to ensure effective detection, response and compliance.

Balancing Manual and Automated Fraud Prevention Approaches

Organizations continue to blend manual oversight with automated tools, reflecting the need for both strategic intervention and technological efficiency in fraud prevention. A balanced mix of manual and automated processes remains the most common approach, particularly in Canadian retail and U.S. retail. U.S. and Canadian ecommerce segments report higher reliance on mostly automated fraud prevention strategies compared to retail. Few organizations rely entirely on automated fraud prevention, with only 3%-6% in any segment indicating full automation.

Businesses must refine their fraud prevention frameworks to maximize efficiency while maintaining necessary manual intervention for high-risk scenarios. Retailers may need to adopt more automation to enhance fraud detection scalability, while ecommerce firms should ensure human oversight to mitigate evolving fraud tactics.[4]

Organizational Approach to Fraud Prevention



Question(s) 40

4: https://risk.lexisnexis.com/global/en/insights-resources/white-paper/securing-today-innovating-for-tomorrow-responsible-ai

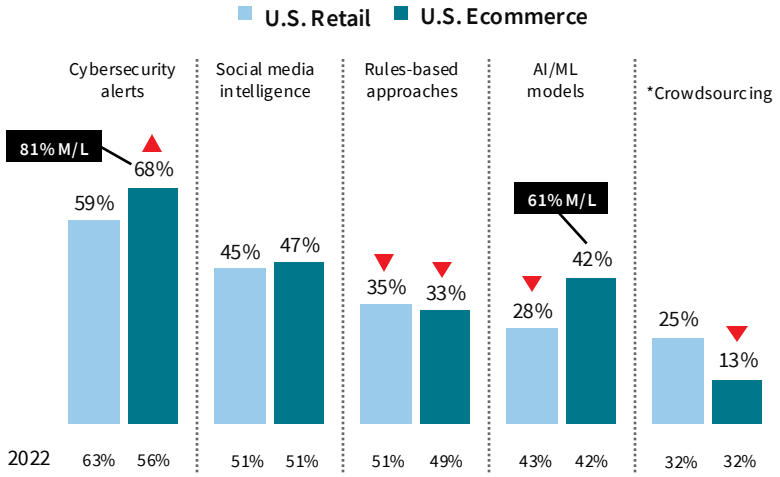
Expanding Use of Supportive Capabilities in Fraud Prevention

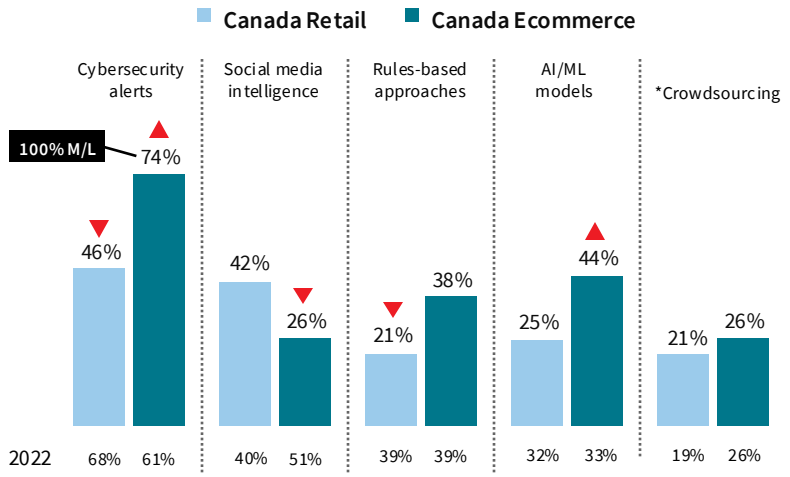
Organizations are leveraging a mix of cybersecurity alerts, AI/ML models, social media intelligence and crowdsourcing to strengthen fraud detection and response efforts. However, reliance on specific capabilities varies across regions and industries.

Cybersecurity alerts are the most widely used tool across all segments, with the highest adoption in Canadian ecommerce (74%) and U.S. ecommerce (68%).

The continued dominance of cybersecurity alerts reflects an industry-wide push for proactive fraud detection, yet gaps in AI/ML adoption may slow innovation for some segments. A report by the Congressional Research Service highlights that while AI can enhance fraud detection, its adoption introduces challenges and risks, including potential biases and the need for substantial data infrastructure.[5]

% Using Supportive Capabilities to Fight Fraud





Cybersecurity solutions protect systems, networks and data from breaches, hacking and cyber threats using tools like firewalls, encryption and threat intelligence.
Fraud prevention solutions detect and stop fraudulent activities in transactions, identities and accounts using behavioral analytics, identity verification and risk scoring.

▼▲ = significantly or directionally higher/lower than previous period

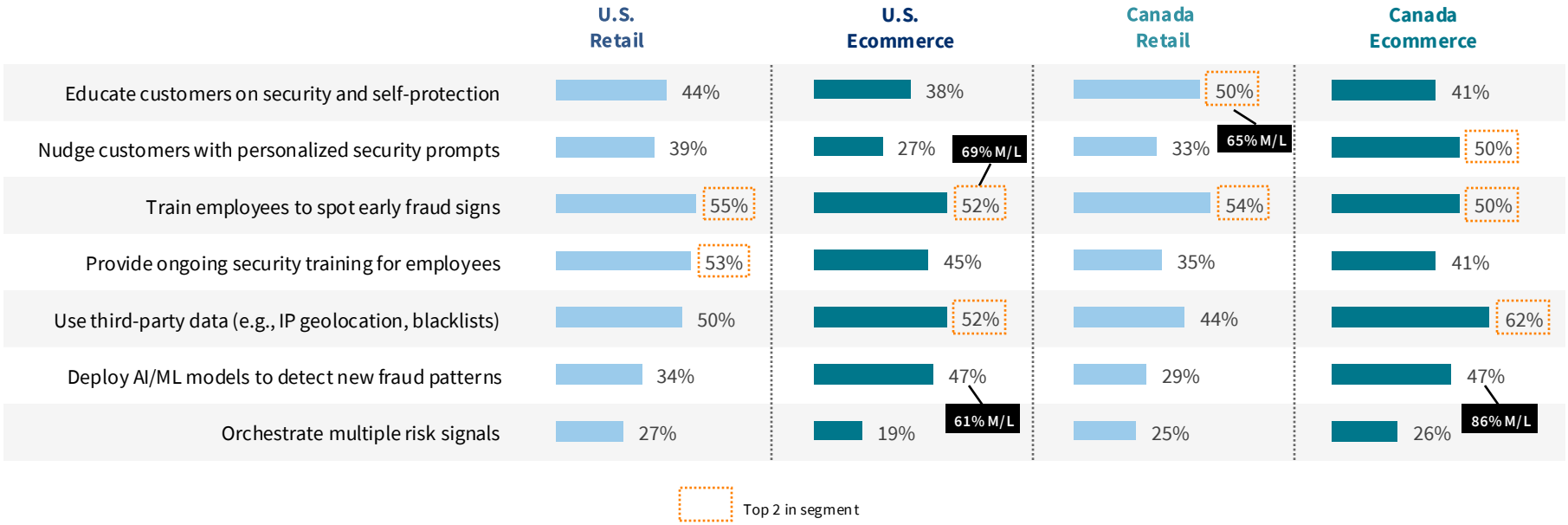
Question(s) 30C

5: https://crsreports.congress.gov/product/pdf/R/R47997

Organizations are reinforcing their scam mitigation strategies through a combination of employee training, customer education and advanced AI-driven detection.

Organizations are combining employee training, customer education and AI-driven detection to fight fraud, but the challenge lies in maintaining security without adding too much friction. Training employees to recognize fraud early and using proactive customer engagement—such as personalized security prompts—help mitigate scams without overwhelming users. At the same time, AI/ML solutions play a growing role in detecting fraud patterns while allowing for a smoother, more seamless customer experience.[6]

Scam Mitigation and Prevention Measures



Question(s) 22C

6: https://risk.lexisnexis.com/insights-resources/white-paper/defend-against-authorized-transfer-scams

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.

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.

Recommendation #1

Combine a risk-based and data-driven approach with multilayered fraud solutions. To better identify patterns and anomalies in customer behavior, leverage technology such as advanced user profiling and scale assessment with responsibly driven AI. 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 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.

MULTILAYERED 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 collaborative risk intelligence for additional insights.

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, a physical device in the user's possession or automated document authentication.

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

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.

Protect Entry Points

To reduce drop-off rates and provide secure, seamless and accessible onboarding the moment consumers walk in the door, verify biometrics and authenticate documents in under 30 seconds.

This helps guard against attacks while improving the customer experience.

MULTILAYERED SOLUTIONS APPROACH

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.

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.

- Single point protection is no longer enough and results in single points 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 multilayered, 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, across industries and countries, is essential for identifying risks and mitigating more account takeover attacks.
- Enabling integrated forensics, case management and business intelligence can help to improve productivity.

LexisNexis® RISK SOLUTIONS

Appendix

Survey Questions

Survey Questions

S9. Which of the following ranges best describes your company's annual revenue, in USD? Please consider total revenue from all sales channels and locations.

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

Q2. When making decisions about fraud prevention and customer experience, which of the following priorities is most important and least important to your organization?

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

Q3c. What are the primary factors that contribute to abandonment during the following customer journey stages?

Q4. Has your organization experienced measurable changes in customer churn directly attributable to fraud prevention measures over the past 12 months?

Q10a. Keeping in mind the definition previously shown, which of the following best captures the approximate dollar value of your company's total fraud losses (in USD) over the past 12 months?

Q10b. Approximately, how much of your fraud losses would you attribute to each of the customer journey stages: new account creation (fraudulent new accounts), purchase transactions and account login/security (i.e., related to account takeover)? To answer this, please distribute 100% across each of these customer journey stages.

Q11a. Now, continue to think about these three customer journey phases separately and your organization's fraud losses during the past 12 months. For each specific customer journey stage, please indicate the percentage distribution of your past 12-month's fraud losses across the following fraud methods. Please estimate to the best of your knowledge.

Q11b. For identity-related fraud, what is the distribution by the following types of activities?

Q14. Please indicate the percent of fraud costs generated through each of the following transaction channels currently used by your company (as a percentage of total annual fraud losses). Please estimate to the best of your knowledge.

Q15a. Think again about the fraud losses your company suffered during the past 12 months. Please estimate the percentage distribution of various direct fraud costs (direct and indirect) that occurred during the past 12 months for each of the channels listed.

Q17. In thinking about the total fraud losses suffered by your company during the past 12 months, please indicate the distribution of various fraud costs for each of the payment methods used by your company. Please estimate to the best of your knowledge.

Survey Questions

Q20. Please rank the top three challenges related to fraud your company faces when selling to customers online and via mobile.

Q22. What steps have your organization taken to mitigate and prevent scams?

Q29a. In a typical month, what percent of your transactions are determined to be malicious automated bot attacks (i.e., rapid creation and placement of hundreds of orders/transactions by fraudulent automated bots at the same time)?

Q29b. How does this compare to the same time last year? Would you say the percent of monthly automated malicious bot attacks has…

Q30. Which fraud detection/mitigation solutions does your company currently use for the following transaction or customer journey points? Please select all that apply.

Q30c. In addition to solutions, what supportive capabilities is your company using to help fight fraud?

Q31. What are the top five most important features in a fraud-management solution?

Q32. To what extent does your organization use machine learning-based approaches to prevent or mitigate the following fraud types?

Q34. To what degree is your company focused on minimizing customer friction during an online or mobile channel transaction checkout?

Q35a. To what degree is your company focused on minimizing customer friction when someone opens a new account online or through a mobile device?

Q40. How would you describe your organization's approach to fraud prevention?

Q42. How would you rate the effectiveness of your organization's fraud detection and mitigation efforts?

Q43. How would you characterize your organization's outlook for being able to detect and mitigate fraud during the next 12 months?

Q44. How do you expect your organization's spending on fraud prevention and mitigation to change during the next 12 months?

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 http://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.