

Retail and Ecommerce



Understanding fraud's true impact on ecommerce and retail is a first step toward improving outcomes for businesses and customers.

Contents

- 4** Business growth and customer experience pressures complicate effective fraud control

- 6** Fraud drives rising costs beyond losses, even when prevented

- 8** Fraud risk is fragmented across channels, types and touchpoints

- 10** Fraud prevention is shifting towards integrated, multi-layered defenses

- 12** Investment in fraud management solutions is rising, but execution presents major hurdles

- 14** Agentic commerce is expanding faster than organizations' ability to manage its fraud risk

- 16** Fraud management maturity drives stronger outcomes and experience alignment

- 18** Building a successful strategy to mitigate fraud



Ecommerce and retail companies are diversifying their investments in fraud prevention to stay ahead of this fast-changing landscape.

Retail and Ecommerce

Companies struggle to advance growth priorities as anti-fraud efforts compromise customer experience

Providing the frictionless experiences today's customers demand while keeping fraud at bay is a serious challenge. As transaction fraud grows more complex (including new security concerns introduced by agentic commerce) and more expensive, across North America and around the world, smart anti-fraud efforts and investments are paying off.

LexisNexis® Risk Solutions created this report to understand how retailers and ecommerce companies across North America are meeting this moment. Here's what we found:

Higher-maturity businesses that prioritize improving customers' digital experiences and integrate those experiences with fraud prevention efforts are dramatically improving their effectiveness.

They're simultaneously preventing more fraud and decreasing customer churn, sometimes quite dramatically.

We collected data for this report in 2025 and 2026, from 513 risk and fraud executives representing ecommerce and retail companies in the U.S. (437) and Canada (76). Just over half of these respondents (292) represent small companies earning less than \$10 million in annual revenue; the remaining 221 are mid-size and large companies earning \$10 million or more per year. The study considers only consumer-facing fraud, not insider or employee fraud.

Data highlights include:

- Organizations face widespread, complex and layered fraud risks.
- These risks span all channels, payment methods and stages of the customer journey.
- Financial impacts extend far beyond direct losses to include operational, legal and reputational expenses.
- Companies are increasing investment in fraud prevention solutions.
- Successful strategies combine identity, device, behavioral and other signals in integrative, adaptive and experience-driven anti-fraud solutions.
- Concern is growing around increasing exposure to risk driven by the rapid adoption of agentic commerce.

Read on for the details.

37%

of North American retail and ecommerce companies were significantly impacted by fraud-related revenue losses this year.

Business growth and customer experience pressures complicate effective fraud control

For retail or ecommerce platforms, keeping customer interactions free of unnecessary friction is critical for growth. The risks posed by today's complex, AI-scaled fraud schemes exacerbate this challenge. To meet business goals, North American retail and ecommerce organizations have to find ways to secure transactions without negatively impacting customer experience.

When asked what priorities would drive their business initiatives in the next year, about half of retail and ecommerce companies in the U.S. and Canada cited improving customer experience and boosting bottom-line performance as top priorities. (See Fig. 1.) Building top-line growth was the top priority for Canadian ecommerce businesses. Improving fraud management and prevention was the No. 3 priority for Canadian retailers, a concern shared by more than half of U.S. retailers. U.S. ecommerce businesses worried about chargeback fraud, too.

Sellers Prioritize Loyalty, Profitability, and Fraud Management

Fig. 1 Business objectives considered high priority (top three answers)



U.S. Retail

57% Improve customer experience and loyalty

53% Improve fraud management and prevention

51% Improve bottom-line performance

U.S. Ecommerce

51% Improve bottom-line performance

47% Improve customer experience and loyalty

42% Reduce chargebacks/chargeback fraud



Canada Retail

63% Improve customer experience and loyalty

60% Improve bottom-line performance

56% Improve fraud management and prevention

Canada Ecommerce

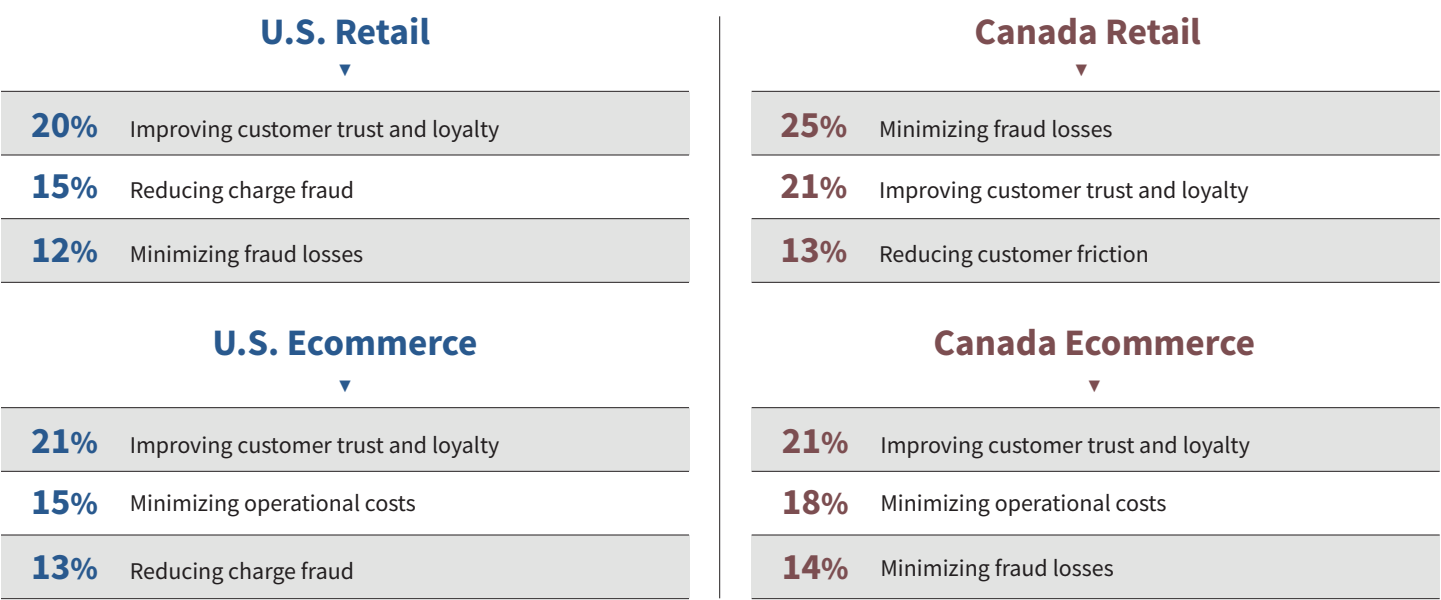
64% Build top-line growth

61% Improve fraud management and prevention

54% Improve customer experience and loyalty

Shaping Customer Trust Through Seamless Experiences A Top Priority

Fig. 2 Main priorities for fraud prevention and customer experience (top three answers)



Retailers and ecommerce providers must find ways to secure transactions online without scaring customers away. In the face of this challenge, what tactics are they prioritizing? Our data shows that focusing on seamless experiences that build customer trust and loyalty is a top priority across the board, cited by around a fifth of retail and ecommerce platforms across North America. For U.S. retailers, reducing charge fraud was their second highest priority; for U.S. ecommerce companies it was minimizing operational costs. In Canada, one in four retailers named minimizing fraud losses their top priority. (See Fig. 2.)

The tension between the need to tighten fraud defenses and the need to keep customer experiences smooth isn't just theoretical. Our data reveals a direct impact of increased fraud prevention efforts on customer churn in North America. 56% of U.S. retailers and 54% of U.S. ecommerce companies said they'd experienced increased customer churn over the last year thanks to anti-fraud measures; in Canada the figures were 40% of retailers and 29% of ecommerce firms. Across the region, the struggle to balance strong fraud protection with smooth and productive customer experiences is ongoing.

>\$5

The fraud multiplier now exceeds \$5 for North American retail and ecommerce companies, for the first time ever.

Fraud drives rising costs beyond losses, even when prevented

Fraud-related revenue losses were cited as a significant business impact by 40% of U.S. retailers, by 36% of U.S. ecommerce merchants, and by less than a third of their Canadian counterparts. However, the economic damage that fraud inflicts can often be significantly higher than the value of the fraudulent transactions. Even when businesses are successful in fighting fraud, they can still absorb significant financial losses from indirect costs like regulatory fines, reputational damage, new compliance requirements, and more. We track this impact every year by calculating the LexisNexis Fraud Multiplier™, the total amount each dollar of direct fraud losses costs once all the associated and indirect costs are added up.

This value has risen steadily over the last decade. In 2016, the total cost to U.S. retail and ecommerce companies was around \$2.40 for every \$1 of direct fraud loss. This year that multiplier is \$5.13. In Canada, the fraud multiplier was \$2.87 back in 2020, but has risen to \$5.23. This marks the first time either country has seen the fraud multiplier cross the \$5 barrier. (See Fig. 3).

The increasing volume of fraud means retail and ecommerce platforms must shoulder growing downstream costs. The activity required to block this fraud at scale creates a significant ongoing operational burden. And some frauds inevitably do succeed even in the face of a company's best efforts, adding their direct costs to the growing indirect costs of securing the enterprise.

The damage is particularly significant in U.S. retail companies. Each blocks an average of more than 600 fraudulent transactions per month, with an average transaction value of \$6,297. However, more than 600 successful fraudulent transactions occur during the same time frame, with an average transaction value of \$5,281. Canadian retail companies block more than 400 transactions (averaging \$4,119 each) and fail to block about 400 (averaging \$5,835 each) during the same period. Damage to ecommerce companies is less, but still significant, with U.S. companies logging an average of \$1,829 per transaction in direct damages from successful fraud and Canadian companies absorbing an average of \$442 per transaction.

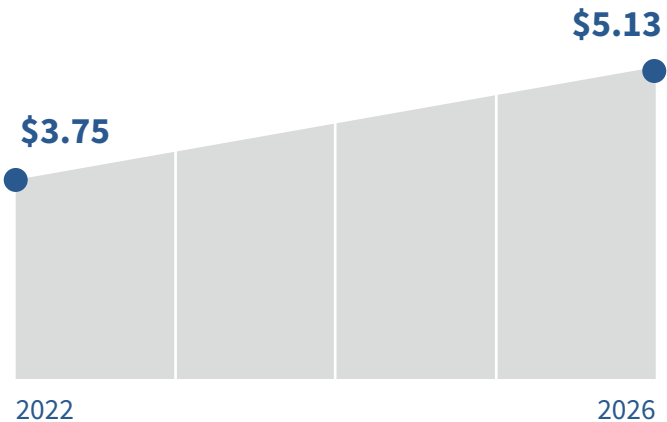
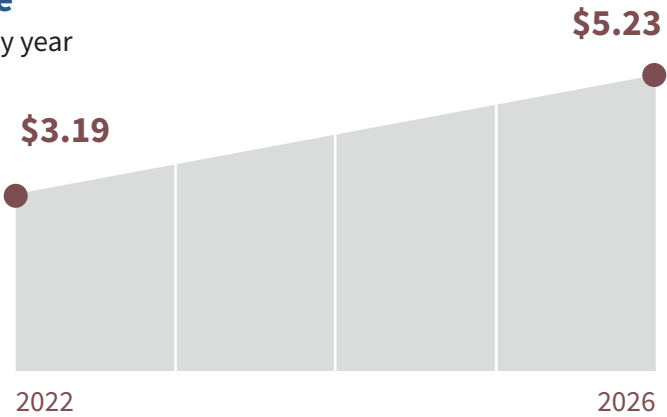
Multi-layered anti-fraud strategies help organizations reduce operational burden, control downstream costs and strengthen security at scale.



The Total Cost of Fraud Now Exceeds 5x the Value of Financial Losses, and Continues to Rise

Fig. 3 LexisNexis Fraud Multiplier™ for North America, by year

Fraud is getting more expensive—fast. In 2026, the LexisNexis Fraud Multiplier™ value rose across all segments, now averaging more than \$5 for every \$1 of fraud loss. This figure includes not just direct losses, but fraud’s escalating downstream financial impacts across operations, compliance and customer trust.



Over 2/3 of fraud costs are domestic transactions; the remaining 1/3 are cross-border.

Fraud risk is fragmented across channels, types and touchpoints.

The increasingly complex nature of global commerce spreads the risk of fraud across every channel, payment method and customer journey stage. Merchants must increasingly contend with a wide array of overlapping fraud types, including chargeback fraud, lost or stolen merchandise, and fraudulent return requests. (See Fig. 4.) Fraud that targets mobile transactions continues to grow: many organizations cite increases of 10% or higher in the past 12 months, across mobile browsers, wallet apps and contactless mobile purchases.

Diving deeper into the data (see Fig. 5):

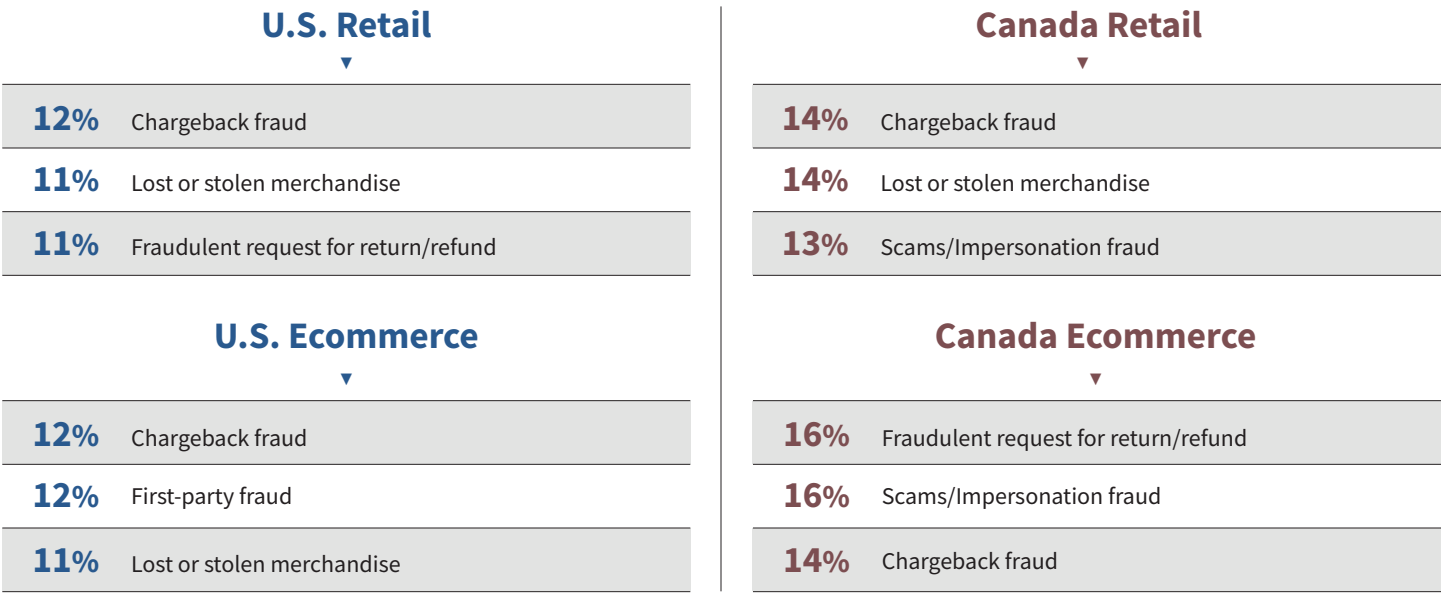
- Domestic transactions still drive from 2/3 to 3/4 of all fraud, but cross-border

- exposure remains material.
- Online and mobile channels account for most fraud costs, apart from Canadian retailers, where about half of fraud takes place in physical stores.
 - Fraud costs are heavily concentrated at the point of purchase, rather than at new account creation or login.
 - Card and digital payments drive the largest share of merchants' fraud costs across North America, with card fraud particularly prominent among Canadian retailers.

This complicated risk environment makes it hard for companies to establish strong fraud controls while preserving a less friction customer experience. The threats companies face today require a fraud defense sophisticated enough to meet the challenge.

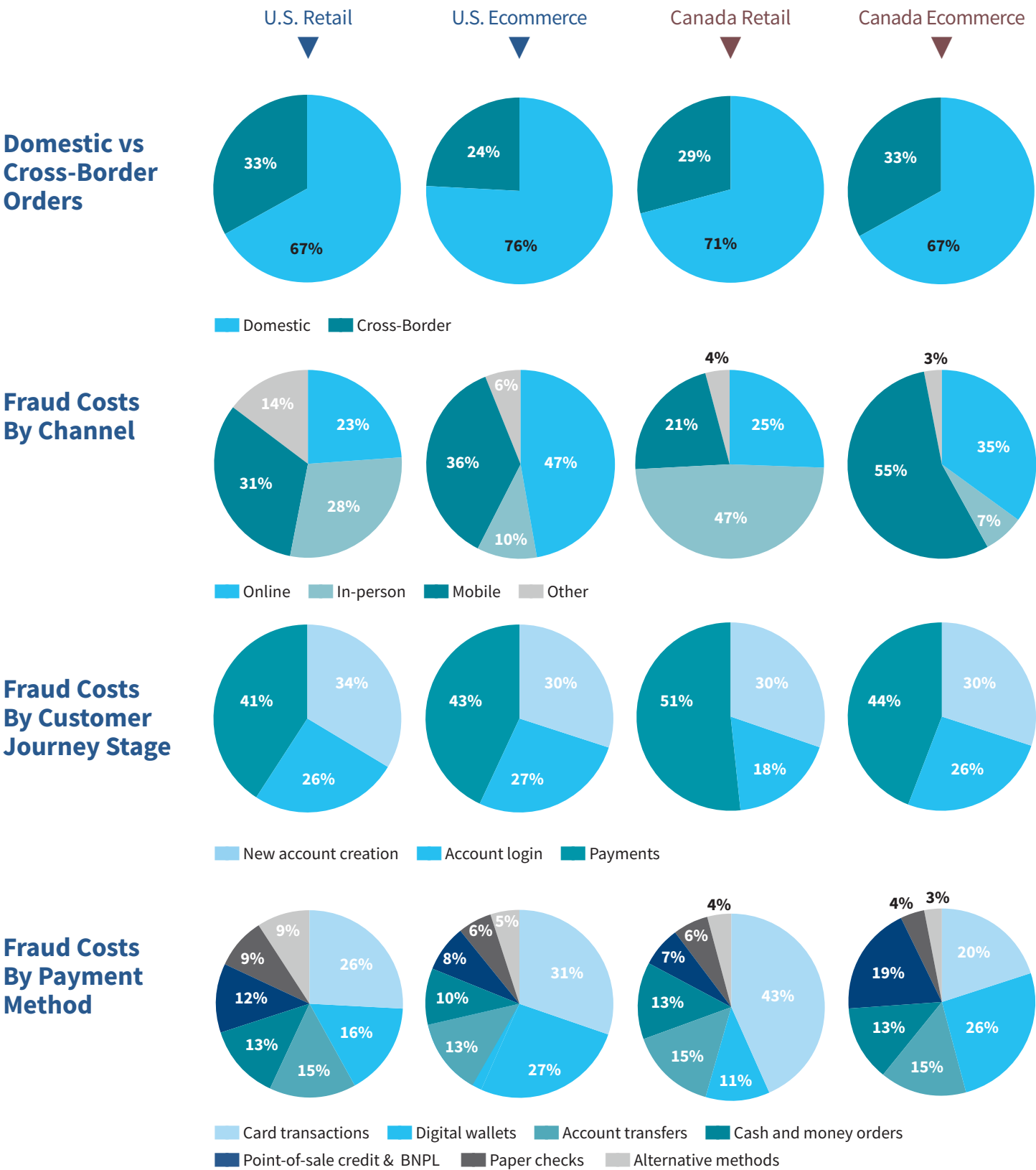
Chargebacks, Stolen Merch, and Fraudulent Returns Are Top Fraud Types

Fig. 4 Distribution of fraud losses, by fraud type (top three answers)



Fraud Costs: A Detailed Breakdown

Fig. 5 Fraud costs measured by order type, channel, customer journey stage, and payment method



Fraud prevention is shifting towards integrated, multi-layered defenses

Ecommerce and retail companies are recognizing that single-point solutions are becoming less effective in the face of modern fraud threats. They're investing in integrated, multi-layered strategies that combine identity verification, behavioral signals, device intelligence and third-party data. These systems will allow them to confidently build unified workflows that mitigate fraud across each customer's entire journey.

The specific mix of fraud mitigation solutions is different for each merchant, but some patterns are emerging. At the new account creation stage, biometric authentication is a top three solution across North America. U.S. merchants also favor email and risk verification, and Canadian merchants lean primarily into real-time transactions tracking tools. At account login, biometric authentication is favored by retailers in both countries, while U.S. ecommerce relies primarily on device ID/fingerprinting and Canadian ecommerce leans more heavily on OTP/2-factor authentication. (See Fig. 6.)

Merchants in North America supplement their multilayered strategies with a range of supportive capabilities, starting with cybersecurity alerts, currently in use at more than 60% of retail and about 50% of ecommerce businesses across the region. Other supportive capabilities cited by our respondents include AI/machine-learning models (more popular in the U.S. than in Canada), rules-based approaches (employed, in Canada, by half of ecommerce companies and 42% of retail businesses) and social media intelligence.

Each of these capabilities can serve multiple purposes within a multilayered strategy. Machine learning, for example, is commonly applied to a wide range of fraud types, particularly scams, lost or stolen merchandise and third-party identity fraud. Between a third and half of U.S. and Canadian merchants apply machine learning to reduce pre-authorization fraud. For post-authorization fraud, it's used by nearly half of U.S. merchants, but fewer than a third of Canadian merchants. About half of respondents in both countries say they use third-party data like IP geolocation and blacklists to help prevent scams; nearly as many invest in employee training to spot early signs of an unfolding scam.

Modern anti-fraud strategies embed AI/ML into layered frameworks, unifying multiple signals and capabilities to drive more accurate decisions and mitigate fraud across the entire customer journey.

Many organizations have begun to shift their prevention strategies for customers using alternative payment methods. This adaptation is more marked among U.S. companies, with 58% of retail and 51% of ecommerce leaders saying that they use significantly different strategies

Biometrics Is the New Norm For Account Creation; Geolocation Shines at Purchases

Fig. 6: Fraud mitigation solutions currently employed (top three for each customer journey phase)

	New Account Creation	Account Login	Purchase Transaction
U.S. Retail	- Email and risk verification - Biometric authentication - Geolocation	- Biometric authentication - Email and risk verification - OTP/two-factor	- Geolocation - Authentication using a payment instrument - Government-issued ID
U.S. Ecommerce	- Browser/malware tracking - Email and risk verification - Biometric authentication	- Device ID/fingerprinting - Geolocation - OTP/two-factor	- Authentication using challenge questions - Name/address/DOB verification - Biometric authentication
Canada Retail	- Real-time transactions tracking tools - Biometric authentication - Geolocation¹	- Biometric authentication - Phone number risk and verification - Check verification services	- Geolocation - Check verification services - Email and risk verification
Canada Ecommerce	- Real-time transactions tracking tools - Biometric authentication - Phone number risk and verification²	- OTP/two-factor - Automated transaction scoring - Name/address/DOB verification³	- Geolocation - Phone number risk and verification - Government-issued ID
¹ Tied for top selection with check verification service ² Tied for top selection with device ID/fingerprinting, geolocation, authentication using quiz and government-issued ID ³ Tied for top selection with browser/malware tracking, authentication using quiz and government-issued ID			

to face the risks involved with these payments, vs. 42% and 46% of Canadian retailers and ecommerce leaders.

Coordinating all this new complexity is another ongoing challenge. More than half of merchants say their cybersecurity operations are only partially integrated with customer experience and fraud

prevention efforts. Full integration is most common among U.S. retailers (39%), and least common among Canadian ecommerce operations (18%). About half of companies in the region believe that tools for fraud-management administrators are an important part of a fraud defense arsenal.

43%

43% of Canadian (and 24% of U.S.) ecommerce merchants plan to add browser and malware tracking to their stacks.

Investment in fraud management solutions is rising, but execution presents major hurdles

For companies trying to thrive in today’s complex fraud environment, investing in fraud detection, analytics and mitigation is mission-critical. Asked what specific solutions they currently plan to tackle in the next 24 months, respondents cited a broad distribution of more than a dozen solutions, naming behavioral biometric authentication and browser/ malware tracking most often. (See Fig. 7.)

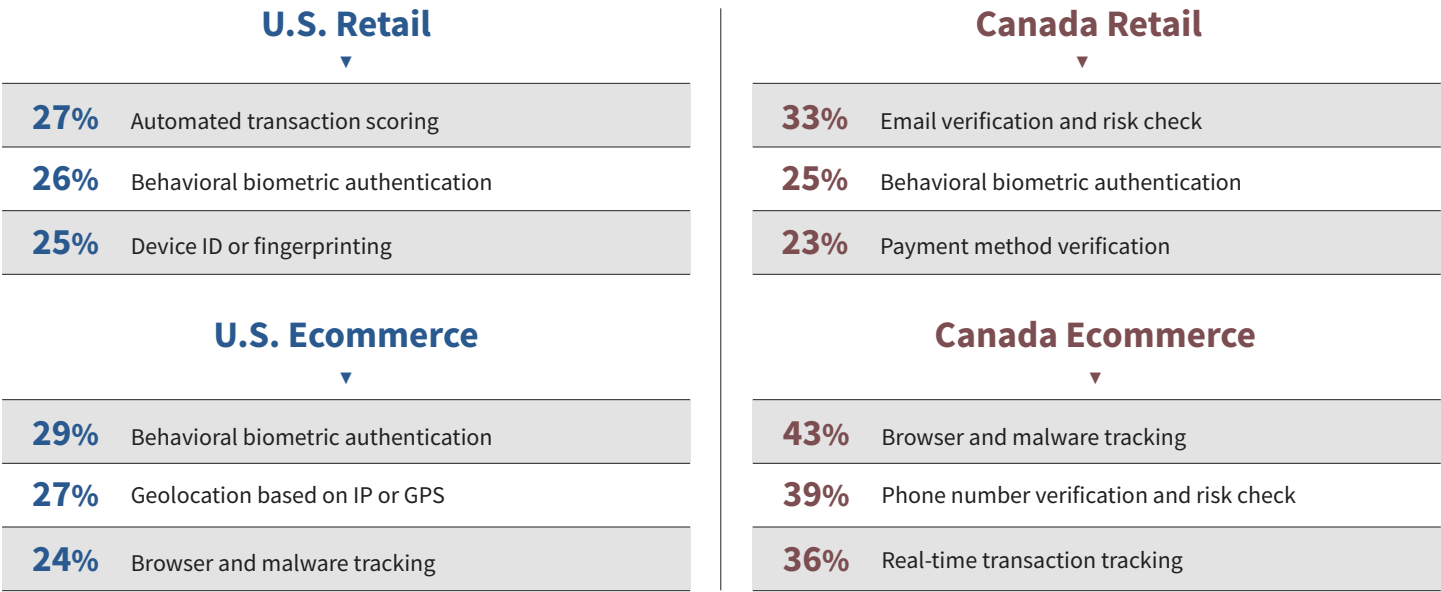
Making sense of all this point solution data is a growing challenge. Retail companies in both countries are more

likely to have larger data science teams helping detect, analyze, and prevent fraud. Almost half (45%) of U.S. retail companies have a data science team of 3 to 5 employees; another 25% have even larger teams. In Canada, just 31% of retailers have a team of 3 to 5 people, and only 10% have larger teams. In both countries, ecommerce teams are even smaller: About 43% of companies rely on just 1-2 experts to fight fraud, and 25% have no data science staff at all.

Across the board, at least two thirds of organizations expect fraud prevention budgets to hold steady or increase over the next year, led by 45% of U.S. retailers who expect their budgets to grow.

Companies Plan To Deploy a Wide Variety of Anti-Fraud Solutions

Fig. 7 Planned fraud solution investments over the next 24 months (top three answers)



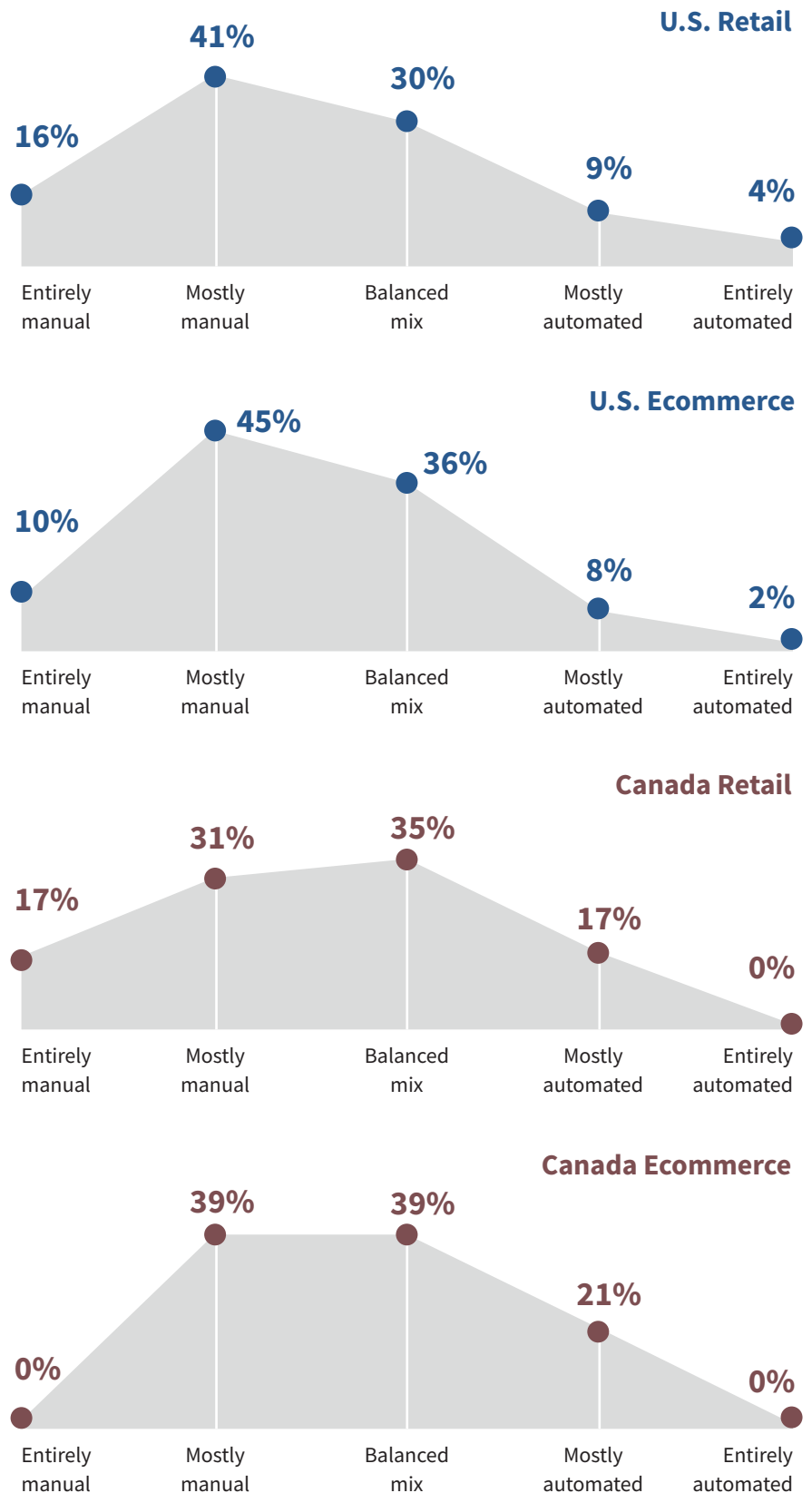
Businesses Begin To Automate Fraud Prevention

Fig. 8 Organizational progress in automating fraud prevention

However, despite these current and planned investments, coverage gaps and inconsistent visibility still plague companies trying to stay ahead of this evolving threatscape. Many are able to track key dimensions of fraud, but their visibility varies. Example: 83% of U.S. retailers, but only 68% of Canadian ones, can currently track synthetic identity fraud separately from credit losses. Similarly, more than 90% of companies across the region are either tracking fraud costs by channel or by payment method, but fewer than half of retailers, and a little over a third of ecommerce merchants, are tracking both.

These organizations' confidence is high: More than 70% of U.S. companies and more than 60% of Canadian companies say they are mostly or extremely confident about their ability to detect and mitigate fraud. They're cautiously automating fraud prevention. (See Fig. 8.) And half or more of these companies, in both countries, say they expect their performance to improve over the next year. Canadian ecommerce merchants show the most optimism, at 79%.

However, this high confidence doesn't seem to be translating into measurably better outcomes yet. Among companies rating their fraud mitigation as extremely or mostly effective, 32% still fall into the high fraud-loss-rate bucket, about the same as companies rating their efforts as somewhat or not effective (31%). This risk of overestimating effectiveness is another major hurdle that companies have to overcome.



73%

73% of U.S. retailers (and 54% of Canadian retailers) are adopting agentic fraud analysts.

Agentic commerce is expanding faster than organizations’ ability to manage its fraud risk

Adoption of agentic commerce is accelerating in the region, allowing AI-powered nonhuman identities to shop, compare prices and services, negotiate and even purchase products on behalf of their customers. Canadian ecommerce and U.S. retail companies report particularly robust adoption (at more than 60%), and other businesses in the space aren’t far behind, with nearly 50% adoption. However, merchants leaning into this promising new technology must also reckon with the new avenues of risk that it opens up.

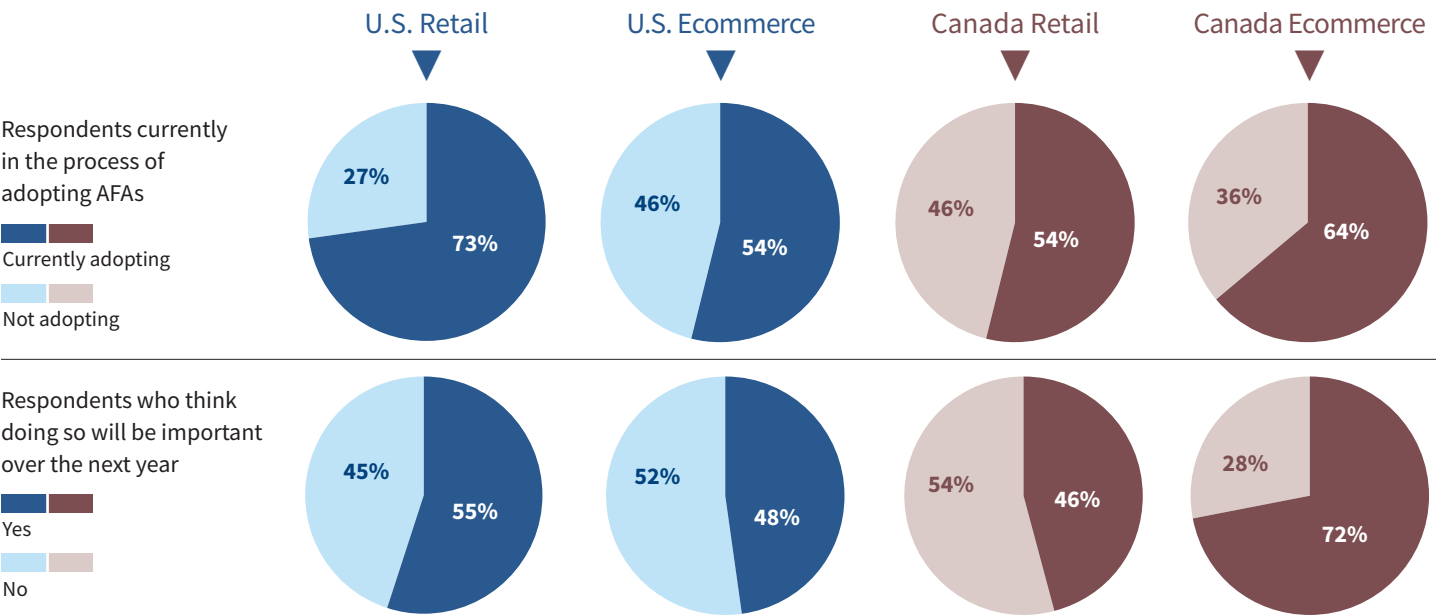
More than half of Canadian merchants, and more than two thirds of U.S. merchants, say they feel either somewhat

or very worried about agentic fraud risk. A wide variety of specific concerns are keeping them up at night. U.S. retailers are most worried (28%) about the challenges of integrating their existing fraud tools with agentic-driven transaction flows, and validating agents’ transaction intent (27%). Ecommerce companies in the U.S. are more concerned about the potential for increased returns abuse and refund fraud (28%), as well as increased chargeback fraud (26%).

On the Canadian side, merchants are also concerned about integrating agent-driven transaction flows into their current fraud-detection tools. Retailers here also worry about a higher risk of account takeover and new difficulties verifying customer transactions (both 27%), while Canadian ecommerce companies are more concerned about

Agentic Fraud Analysts Gain Traction in North America

Fig. 9 Percent adopting AFAs or who think doing so will be very important in the next year



Optimism Rises For Fraud Mitigation Effectiveness

Fig. 10 Effectiveness of current efforts, and improvement expectations

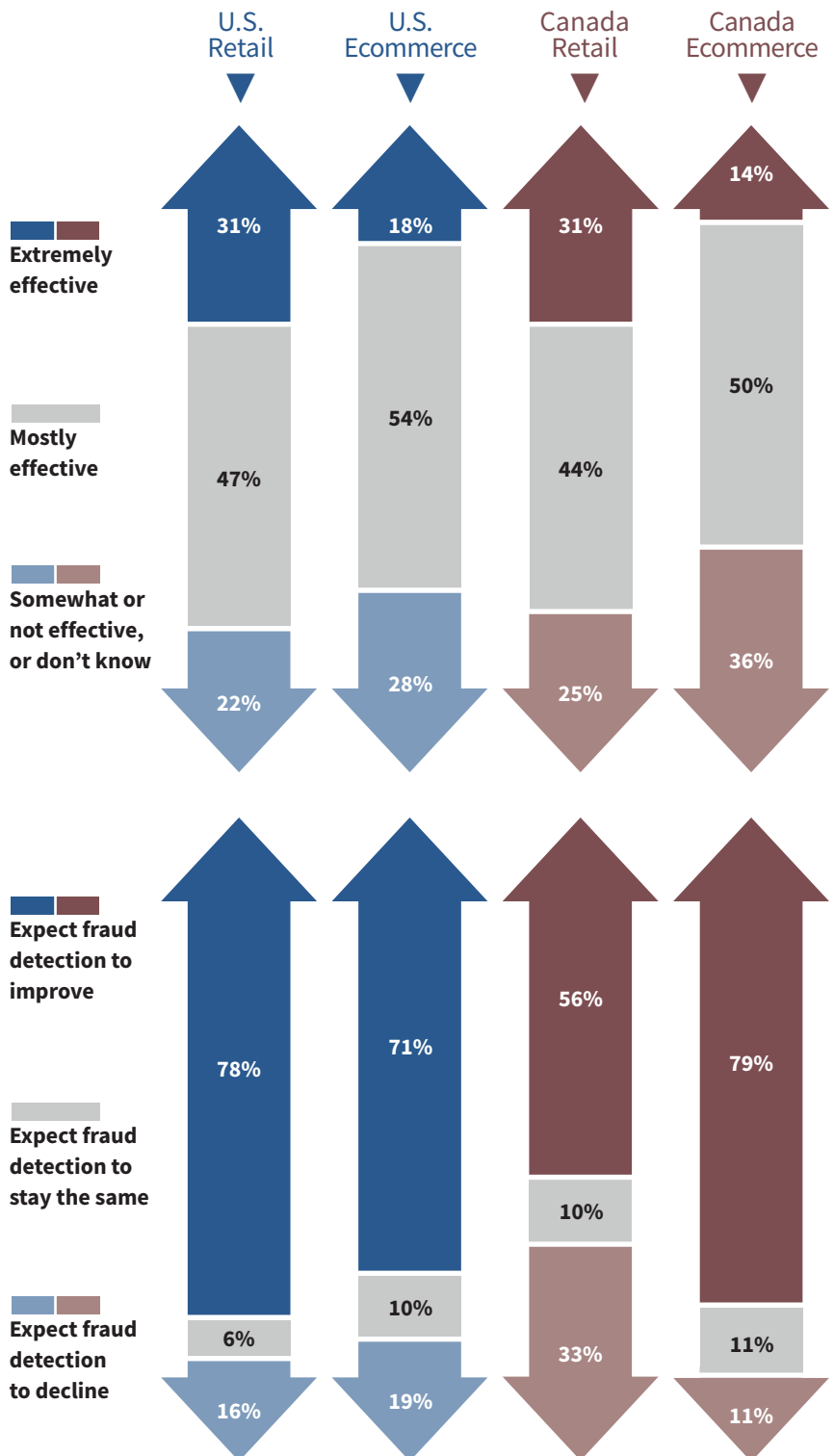
limited visibility into device, network or origin signals associated with autonomous agents (32%) and the difficulty of distinguishing legitimate agent traffic from malicious automated bots (29%).

As a result of these concerns, agentic fraud analyst adoption and investment are gaining traction across North America. (See Fig. 9.) Momentum is strongest in U.S. retail, where 73% are either using agentic fraud analysts now or making the investment, and among Canadian ecommerce organizations (64%).

Faced with all this complexity, just how effective do North American companies think their current mitigation efforts are, and do they foresee fraud detection improving over the next 12 months?

In terms of current practices, retailers in both countries are relatively confident, with 78% of U.S. retailers and 75% of Canadian retailers calling their current activity mostly effective or extremely effective. Ecommerce platforms are a little less confident (72% in the U.S., and 64% in Canada).

Looking to the future, more than 70% of companies across three of the four sectors expect their fraud detection to improve. However, among Canadian retailers, just 56% hold that expectation, and a third actually expect it to decline.



Fraud management maturity drives stronger outcomes and experience alignment

Our final survey questions sought to understand how well the relative maturity of each organization's fraud strategy produced key outcomes those strategies were designed to address.

To set maturity baselines, we assessed how the companies measure, manage, staff, automate and invest in fraud prevention, and looked at factors like tracking sophistication, level of fraud prevention automation, analytics and data staffing levels and expected change in investment. Averaging and combining these numbers produced a single fraud prevention maturity score for each business. Then, armed with those scores (low, medium and high maturity), we looked at their business priorities and their anti-fraud outcomes.

Our data revealed that as companies develop more mature anti-fraud systems, their priorities change. High maturity businesses are more likely to prioritize improving customer experiences, including minimizing checkout friction. They're also more likely to integrate customer experience operations with fraud prevention, and to tighten controls to reduce chargebacks and chargeback fraud. (See Fig. 11.)

It's not just their priorities that change as companies gain fraud prevention maturity: Their outcomes improve as well. A larger share of high-maturity organizations reported decreased customer churn from fraud prevention in the past 12 months (20%, vs. 9% of low-maturity businesses). And they prevent more frauds: Just 4% of low maturity businesses prevent 1000 or more frauds per month, whereas 19% of high maturity businesses do.

Finally, companies with higher fraud-prevention maturity show greater confidence and more optimism that their protective capabilities are effective now and improve over time. Nearly nine out of ten high-maturity organizations expect to improve fraud prevention and mitigation even further over the next 12 months, while only 63% of companies with low maturity predict they'll be able to do so in the same timeframe.

More mature fraud strategies drive stronger business outcomes, reducing customer churn, improving detection effectiveness and aligning fraud prevention with optimized customer experiences.

Fraud Prevention Maturity Guides Strategy and Yields Results

Fig. 11 Business priorities (left) and anti-fraud success (right) as prevention maturity increases

Business Priorities

Improve digital customer experience

39%

47%

Low maturity businesses

High maturity businesses

Accelerate shift to digital business

31%

47%

Low maturity businesses

High maturity businesses

Integrate CX ops with fraud prevention

37%

56%

Low maturity businesses

High maturity businesses

Minimize checkout friction

39%

55%

Low maturity businesses

High maturity businesses

Reduce chargebacks & chargeback fraud

39%

54%

Low maturity businesses

High maturity businesses

Business Anti-Fraud Success

Decreased customer churn

9%

20%

Low maturity businesses

High maturity businesses

Prevented 1000+ frauds per month

4%

19%

Low maturity businesses

High maturity businesses

Prevented 2500+ frauds per month

2%

10%

Low maturity businesses

High maturity businesses

Current anti-fraud effectiveness¹

72%

80%

Low maturity businesses

High maturity businesses

Near-future expectation of improvement²

63%

88%

Low maturity businesses

High maturity businesses

¹ Percent of respondents that rate current efforts as “extremely” or “mostly” effective

² Percent that expect their organization’s fraud detection and mitigation to improve over the next 12 months

Building a successful strategy to mitigate fraud

Ecommerce and retail companies in North America and elsewhere face a tough challenge, in which they should harden their defenses against modern fraud in all its complexity without creating undue friction that drives customers away. But our survey data shows that smart, targeted investments, informed adaptation, and multi-layered anti-fraud strategies can improve the security of transactional platforms while maintaining customer loyalty in this challenging sector.

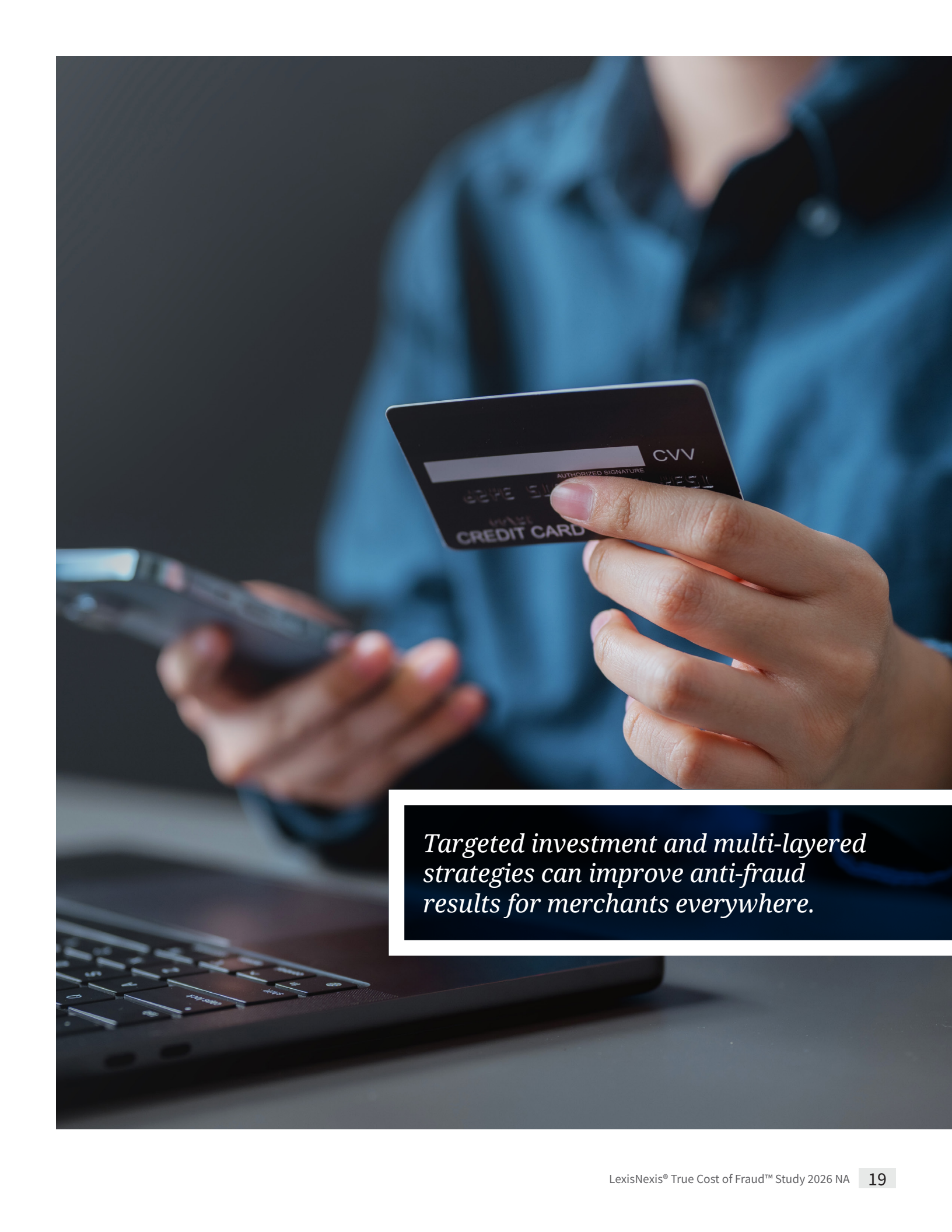
Effective strategies include:

Adopt a complex solution to tackle this complex problem. Point solutions are becoming less effective against modern fraud, and layered approaches are outperforming them. Organizations are finding success today with a layered mix of strategies combining third-party data, device and behavioral intelligence and other tools instead of looking for one silver bullet.

Avoid complacency. The survey shows that even companies that have invested in powerful solutions and have good insights into fraud can report higher levels of confidence than are warranted. The threatscape is in constant motion, and anti-fraud efforts need to do the same, by investing in analysis teams that can intelligently assess current success and prioritize future investments in fraud detection and mitigation.

Prepare (quickly) for agentic AI. The AI revolution, and its effect on commerce, has already begun. Agentic transactions are sure to expand dramatically across the digital space in the months and years to come, making it crucial to apply focus to managing the new risks and complications agentic AI brings.

Build greater anti-fraud maturity. By continuing to fine-tune solutions, including staffing anti-fraud teams and improving tools and processes on a continual basis, merchants can achieve greater anti-fraud maturity and safely grow their businesses in the face of expanding risk.



Targeted investment and multi-layered strategies can improve anti-fraud results for merchants everywhere.



We're on a mission to help people live life more securely. Find out how.

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions provides customers with information-based analytics and decision tools that combine public and industry-specific content with advanced technology and algorithms to assist them in evaluating and predicting risk and enhancing operational efficiency. Headquartered in metro Atlanta, Georgia, the company has offices throughout the world, serves customers in more than 190 countries and territories and is part of RELX. For more information, please visit [LexisNexis Risk Solutions](#).

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis® Risk Solutions products identified. LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.

LexisNexis and the Knowledge Burst logo are registered trademarks and LexisNexis Fraud Multiplier is a trademark of RELX Inc., registered in the U.S. or other countries. True Cost of Fraud is a trademark of LexisNexis Risk Solutions Inc. Other products may be trademarks or registered trademarks of their respective companies.

Copyright © 2026 LexisNexis Risk Solutions.