Deloitte.

Agentic Commerce: Navigating Fraud Risk and Opportunities

Confronting the New Realities of Agentic Commerce and Payments

December 2025

An estimated $17.5 trillion[1] in gross merchandise value is to be unlocked by agentic AI by 2030. As merchants adapt to these shifts in consumer behavior, mitigating fraud risks becomes critical. To assess the impact of the associated increase in AI-enabled fraud has on retail, Deloitte conducted a study across a diverse set of merchants and found that **69% experienced AI-enabled fraud in the past year while only 3% felt well prepared to address increasing attacks enabled by AI**. These findings highlight an urgent need for merchants to adopt proactive and holistic fraud strategies – not only to future-proof their operations but also to enable the capture of the rapidly expanding customer value driven by agentic AI.

Key Takeaways

Agentic AI Adoption

37% increase in fraud from Q2 2025 to Q3 2025 for merchants with notable volume of AI referred traffic[2]

In Q3, it has been observed that the *traffic from* ***GenAI-powered tools is more risky than regular search engine initiated traffic and up to 1.7 times*** *more likely to be fraudulent*[2].

Evolving Threats

87% of merchants in Deloitte survey expect moderate to high increase in AI-enabled attacks in the next 12 months

As "Fraud-as-a-Service" becomes more prevalent, barriers to conduct sophisticated fraud attacks will reduce significantly, leading to not only financial losses for merchants but also ***undermined growth and eroded customer value and loyalty.***

Strategic Priorities

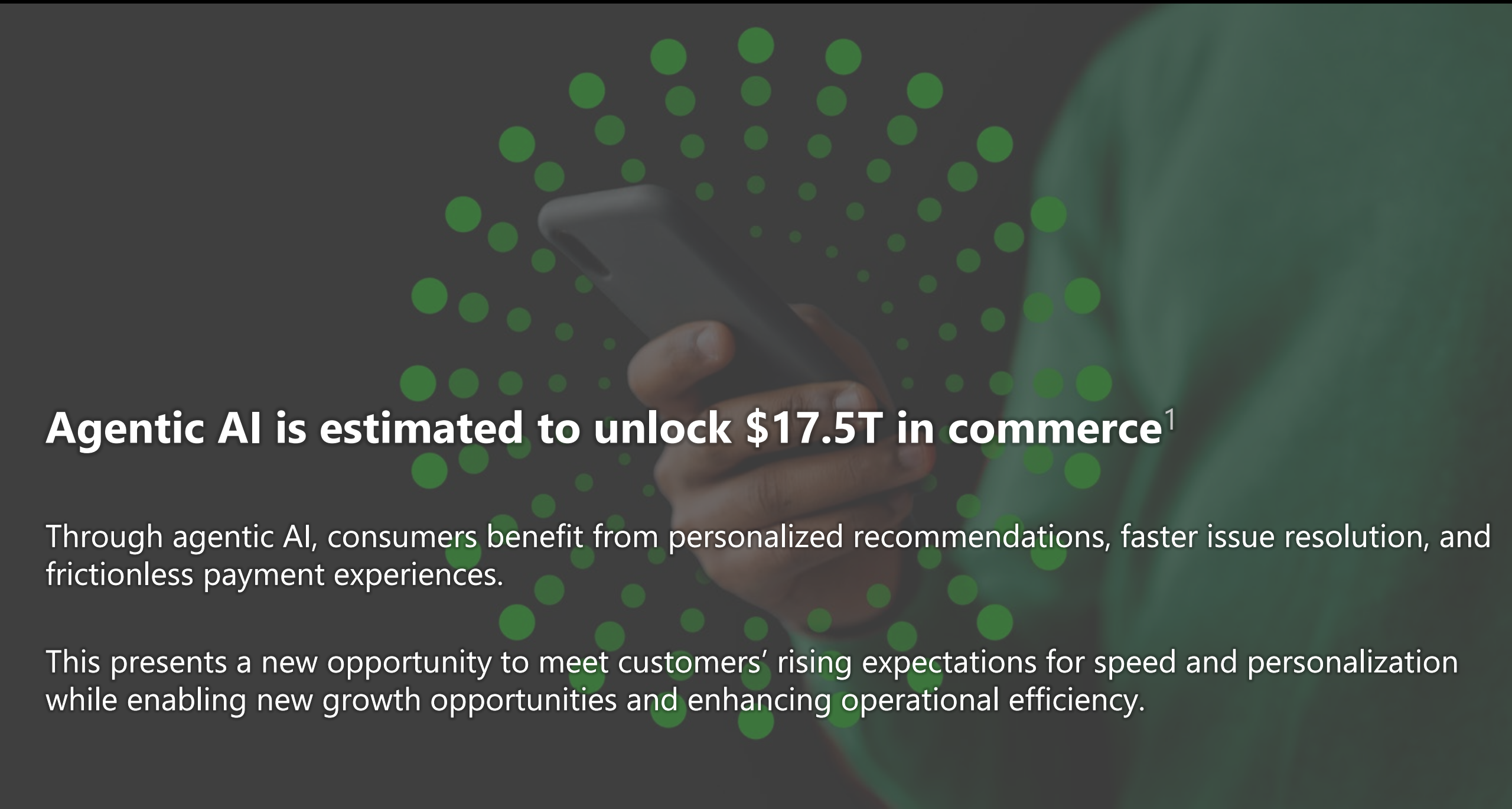
95% of merchants in Deloitte survey are planning to adapt their fraud strategy to consider agentic AI as a strategic priority

While the majority of surveyed merchants (82%) believe advanced analytics to be most effective in mitigating risks, a holistic approach focused on key fraud pillars ***across all customer touchpoints will be paramount in supporting an agentic AI strategy.***

Overcome Obstacles

52% of merchants in Deloitte survey cited funding as the top challenge, followed by resource skillsets, and technology limitations

A strong alignment between ***business and operation KPIs*** *with* ***fraud management KPIs*** *to drive innovative and customer-centric growth will help overcome these barriers.*



Agentic AI is estimated to unlock $17.5T in commerce[1]

Through agentic AI, consumers benefit from personalized recommendations, faster issue resolution, and frictionless payment experiences.

This presents a new opportunity to meet customers' rising expectations for speed and personalization while enabling new growth opportunities and enhancing operational efficiency.

Agentic commerce refers to AI-powered shopping experiences where autonomous agents act on behalf of consumers – searching, comparing, and purchasing products based on consumer preferences and contextual data gathered through prompts. Agentic payment complements this by enabling transactions with built-in mandates and authorization, creating a frictionless end-to-end purchasing process. As consumer adoption accelerates, merchants must undergo significant transformations, including reimagining engagement models, prioritizing personalization, and integrating intelligent systems that meet the consumer demands.

70%

consumers comfortable with AI agents making purchases for them[3]

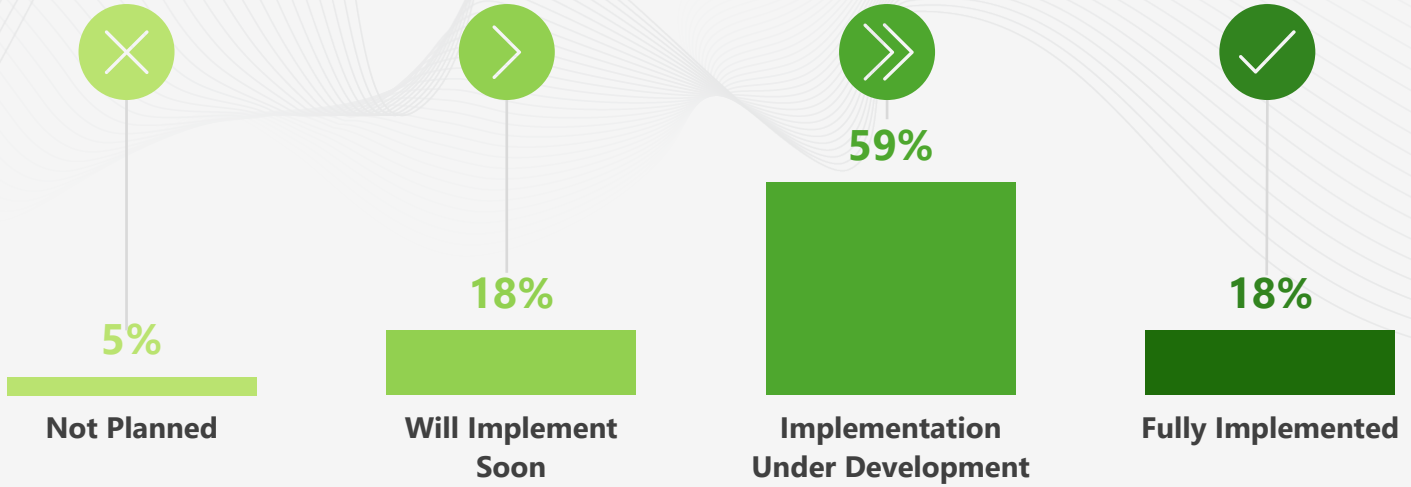
3X

increase in GenAI-driven merchant orders from Jan-Sep 2025[4]

30%

projected digital commerce transaction value influenced by agentic AI by 2030[1]

59% of merchants stated that they have embarked on this journey of agentic AI adoption, with 18% of them believing that they've fully implemented agentic AI capabilities



While agentic commerce and agentic payments are rapidly gaining traction among consumers, the underlying technology also introduces new dimensions of fraud risks. **Agentic AI can function as turnkey engines for AI-enabled fraud attacks** - autonomous systems capable of executing complex sequences of action, making them powerful tools for fraudsters. The very features that enhance customer experience, speed, and minimal human oversight can be exploited to bypass traditional fraud controls. As adoption accelerates, merchants must recognize that the risk landscape is evolving and implement proactive and AI-enabled fraud prevention strategies to safeguard trust and protect revenue.

Evolution of Fraud Risk Landscape Through AI Innovation

2023:
Rise of Gen AI

Explosion of LLM tools such as ChatGPT

2024:
Emergence of Agentic AI

Early solutions with autonomous actions and LLM integrations

Pre-Agentic Era Fraud Attacks

- LLMs democratized fraud knowledge / skills but attacks still **required human execution.**
- Attack sophistication increased, but **orchestrating** and **repeating tasks were still limited by human actions.**
- GenAI streamlined phishing, deepfakes, and synthetic identities, but **adapting attacks to defenses still required human observations and modifications.**

2025:
Adoption of AI Agents

From Jan 2025 to Aug 2025, agentic traffic grew by more than 1,300%[5]

Agentic AI Era Fraud Attacks

1. **Autonomy**
   Multi-step fraud schemes can be **autonomously planned and executed** with minimal input.
2. **Scalability**
   Automated tasks can be repeated easily.
3. **Adaptability**
   Tactics can adapt and evolve to find and exploit **vulnerabilities in new defenses**.

37%

increase in fraudulent traffic from Q2 to Q3 2025 for merchants with a notable volume of LLM-referred orders[2]

110%-170%

riskier than human-initiated traffic observed in Q3 2025[2]

> Agentic AI will be used for "generating fake reviews, affiliation exploitation, [and to] exploit customer service policies."
>
> *– Vice President, Digital/e-Commerce Operations, North American Enterprise Retailer*

In the past year, merchants experienced a variety of AI-enabled fraud attacks, signaling a change in the threat landscape with the rise of Agentic AI. Looking ahead, most merchants expect **fraud risks to continue to increase** as threat actors increase their usage of agentic-AI tools.

69%

of merchants reported experiencing AI-enabled fraud in past year

Over the past year, survey respondents experienced these AI-enabled attacks:

- Deepfake vishing targeting senior executives
- AI-powered chatbots impersonating customer service agents and voice cloning to deceive employees
- Spear phishing campaigns leveraging LLMs
- Automated attempts to purchase using fraudulent credit cards and synthetic identities
- Coupon / promotion abuse with fabricated identities

More agent attacks to come

As "Fraud-as-a-Service" driven by agentic AI becomes more common, these attacks will become more prevalent, automated, adaptive, and damaging, reinforcing the urgency for robust and adaptive fraud prevention strategies to limit impacts.

87%

of merchants expect an impactful increase in AI-enabled attacks in the next twelve months

Top AI-enabled fraud risks that will be further amplified by agentic AI in the future highlighted by survey respondents:

- Synthetic Identity Creation
- Deepfake Social Engineering
- Automated Phishing
- Payment / Card Fraud
- Loyalty Program/ Rewards

AI-enabled fraud presents a multifaceted threat to merchants, impacting everything from **financial performance** and **operational efficiency** to **customer trust** and **long-term growth**.

Addressing these risks is no longer optional, and merchants must safeguard their brand, reputation, and future success.

Wasteful and Fake Traffic

AI-enabled attacks create significant waste by generating high human-like engagement volume and traffic that not only inflates marketing spend as companies pay for impressions, clicks, but also leads not created by genuine prospects and customers. Additionally, the surge in bot-driven traffic can drive website infrastructure usage and increase costs without any corresponding business value.

Disrupted Operations

The rising complexity and frequency of AI-enabled fraud require greater investment in detection and response, straining operational resources and disrupting business processes. This diverts focus from core customer activities and adds constraints to the execution of growth strategies (e.g., restrictions on promotions).

Damaged Loyalty

AI-enabled fraud attacks threaten customer trust and brand reputation through compromised security. By layering on additional static fraud controls, such as added verification steps, customer experience will be impacted negatively with added friction and may diminish long-term loyalty and value.

> “Biggest impact will be to make it hard to distinguish fraud from normal operations”
>
> *– Senior Information Technology Officer, North American Enterprise e-Commerce Merchant*

Deloitte's study finds that, although **67%** of respondents have updated their fraud strategy or implemented new controls, only **3% of the respondents feel 'very prepared'** to handle increasing AI-enabled fraud in the future.

Merchants are not equipped to address the evolving fraud risk landscape with their current control environments. Traditional fraud prevention methods, which depend on predictable patterns and human oversight, are becoming increasingly ineffective against threats posed by generative and agentic AI. These advanced technologies enable attacks to more easily mimic legitimate user behaviors as well as quickly adapt to and exploit static prevention and detection controls on a large scale.

Traditional Controls	Exploitation Methods with AI-Enabled Fraud
Static Authentication	Automates credential stuffing, mines personal data, and can intercept or manipulate basic MFA methods, enabling rapid bypass of static and knowledge-based authentication.
Rule-based Monitoring	Learns and dynamically adapts behavioral pattern to avoid triggering static rules.
Session Information Monitoring / Analysis	Completes sessions much faster than humans, but advanced AI can also mimic human navigation, touchscreen, keyboard and mouse behaviors – making detection increasingly difficult.
Device / IP Blocking	Automates spoofs / changes devices and IP frequently to bypass device / IP blocking.
Manual Review	Overwhelms fraud operations teams with speed and volume, takes advantage of delays in fraud detection and response caused by siloed operations.

Our insights show that **82% of merchants expect advanced fraud detection tools to be the most effective mitigation against AI-enabled fraud**. However, to effectively combat AI-enabled fraud, merchants need to expand their approach across the pillars of fraud management against the speed, scale, and adaptivity of AI-enabled fraud.

Strategy and Governance

Review risk tolerance and ownership by quantifying and tracking exposure from increasing risks and evaluate readiness to adopt new controls to address fraud driven by AI.

Know Your Agent (KYA)

Ensure to detect, classify, and govern all AI agents interacting across channels to prevent AI-enabled fraud and maintain trustworthy interactions and customer experiences.

Adaptive Authentication

Evaluate risk through real-time signals to dynamically tighten verification steps, ensuring that only legitimate users or autonomous agents can access channels or complete transactions.

Dynamic Fraud Detection

Deploy detection tools and/or upgrade analytical rules and models to analyze changing user behaviors and transaction patterns in real time to identify and block fraudulent AI attacks.

Response and Dispute

Ensure effective investigation practices, timely analysis and interventions, and efficient use of resources to address the adaptive and evolving behaviors of agentic AI attacks to minimize financial and operational impact.

Infrastructure and Security

Utilize robust infrastructure and layered security protocols, including access controls and audit trails, as well as advanced data management capabilities, to support the detection of fraudulent agent activities.

To achieve and implement the target state fraud management capabilities, merchants face different challenges, including budget, resource and technology limitations. Among all the limitations, more than half of the respondents believe funding and budget is their number one challenge. With strategic prioritization and expert partnerships, merchants can overcome these barriers and future-proof their fraud defenses while maintaining a customer-centric focus and enabling business growth.

Top Barriers To Implementing Effective Fraud Mitigations

52% **Face Challenges Obtaining Funding/Budget**

38% **Experience Limited Resource Availability/Skill Sets**

34% **Observe Limitation of Existing Technology**

Approaches To Navigate Around The Barriers

Balance Fraud with Customer Experience by aligning fraud management initiatives with e-commerce growth objectives

Expand expert knowledge into the organization through **external partnerships and the use of consortia**

Prioritize High-Impact Use Cases with a balance between "Quick Wins" and Enterprise Transformation

Build internal capabilities through **targeted upskilling** across operations and analytics

Kevin Luh
Fraud Management Leader
Financial Crime

416-824-1663
kluh@deloitte.ca

Shaunna Conway
Offering Leader
Marketing, Commerce & Product

416-807-0611
shconway@deloitte.ca

Andrew J Lee
Partner
Cyber

416-702-5532
andrlee@deloitte.ca

Diksha Pai
Senior Manager
Financial Crime

437-218-6384
dpai@deloitte.ca

David Kao
Manager
Financial Crime

416-202-2891
dakao@deloitte.ca

Eden Sorrell
Senior Consultant
Financial Crime

437-331-6159
esorrell@deloitte.ca

Deloitte's Financial Crime Practice is comprised of seasoned, senior professionals with hands-on, in-depth experience, leading various transformational Fraud initiatives at retail organizations, financial service institutions as well as the public sector.

Deloitte helps clients design, build, and operate dynamic, business-aligned fraud programs for various lines of businesses. You can be assured of being well-equipped to meet the requirements, while continuing to focus on what you do best: managing your organization.

- **Global leadership:** Deloitte is a global leader in Fraud Strategy Consulting. We offer differentiated domain leadership and entrenched industry experience
- **Ecosystems and alliances**: Strong alliances with leading technology vendors, industry organizations, and research entities provide leading insights, intelligence, information-sharing, and collaboration
- **Quantification of fraud risk:** Through integrating data and tailored statistical models for risk quantification, we help organizations to augment their experience with technology to develop risk-intelligence responses
- **Data-driven solutions:** Through our deep technical and industry insight with cutting-edge analytics, we help identify the right data-driven fraud solutions to address the most complex issues impacting your business today

More from Deloitte's Retail Reimagined Series

- **The Future of Stores**
  Connected stores are reshaping retail. Is your organization ready for the store of the future?
- **Retail Loyalty Program Innovation**
  Canadians have high expectations for retail loyalty programs. Are they happy with yours?

Appendix

Summary of Approach and 2025 Deloitte Survey on AI-Enabled Fraud in Retail

Objective

This study was conducted to understand and qualify the shift in the fraud risk landscape with the rise of agentic commerce and payments and to support and equip merchants with an understanding of the increase in AI-enabled fraud risks in agentic commerce and what needs to be considered for the implementation of effective mitigation strategies.

Data Sources

Deloitte conducted a quantitative and qualitative study incorporating a variety of data and expert insights to address key hypotheses on agentic commerce opportunities and impact in retail, incorporating data from partnering solution providers specialized in AI-enabled fraud in the retail ecosystem. This study was conducted from September to October 2025 using a combination of data sources, including:

- ***2025 Deloitte Survey on AI-Enabled Fraud in Retail:*** 39 eligible responses were collected out of a total 62 responses based on the profile of the respondents, including the size of the organization and the respondent's position
- ***Riskified:*** Proprietary e-commerce transaction and fraud attempt data from global merchant network, as well as a 2025 survey of 5,000+ consumers on AI for shopping and agentic commerce risk
- ***HUMAN Security:*** Proprietary digital interaction traffic and research reports across consumer digital journey from ad views, consumption, onsite, and pre/at/post login, including measurements of change in traffic patterns and digital attacks to date

To better understand industry perspectives and challenges related to agentic AI and AI-enabled fraud in retail, Deloitte surveyed 39 North American merchants across various industry verticals. All participants have relevant understanding and experiences with agentic AI, and their organizations reported annual revenues ranging from $1 million to over $100 million.

Respondent Location

92% United States

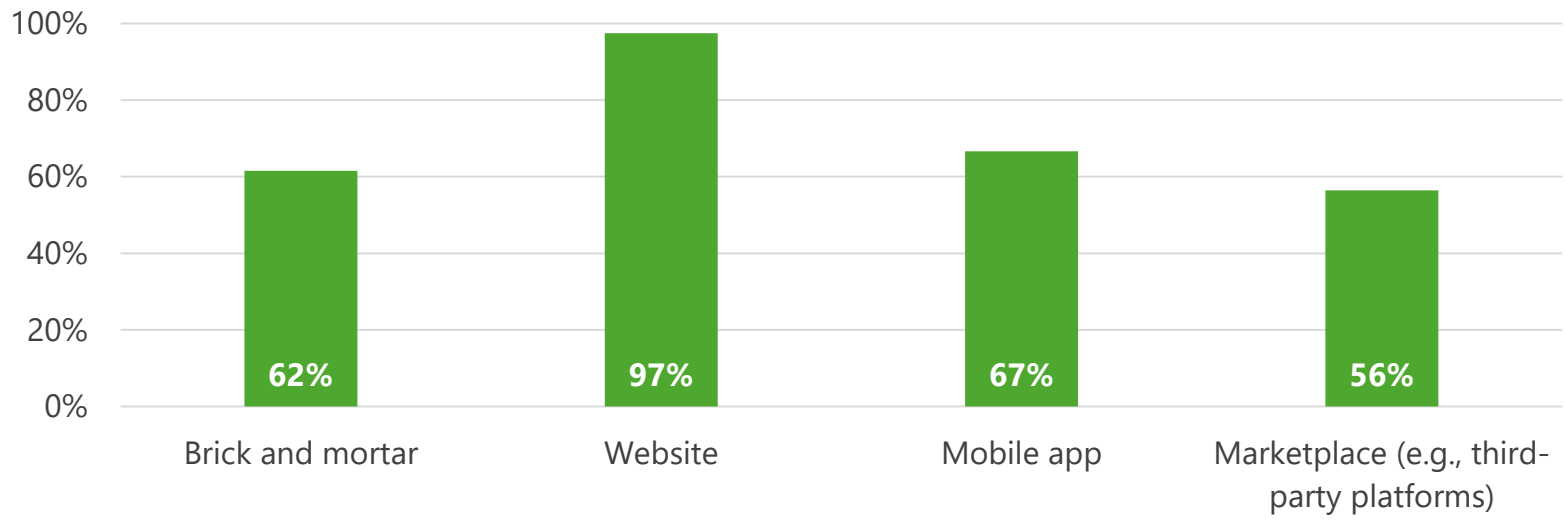
8% Canada

Merchant Annual Revenue	#	%
Less than $1 Million	0	0%
$1 Million to $49.9 Million	2	5%
$50 Million to $99.9 Million	5	13%
$100 Million or more	32	82%

Merchant Industry Vertical	#	%
E-commerce	15	38%
Hospitality	4	10%
Retail	16	41%
Airlines	1	3%
Consumer Services	3	8%

Respondent Organizational Level	#	%
C-level or equivalent	20	51%
SVP-level or equivalent	3	8%
VP-level or equivalent	7	18%
Director-level or equivalent	7	18%
Senior Manager-level or equivalent	2	5%

Channels Used by Merchants



69%

of merchants experienced fraud enabled by AI in past year

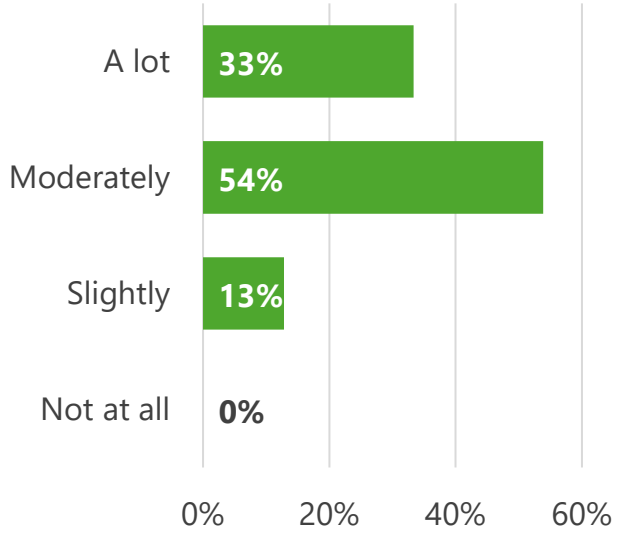
Types of AI-enabled fraud experienced in the past year

- Fake/synthetic identity
- Document fabrications
- Deepfake impersonations
- Phishing/spear phishing
- Social engineering
- Brute force password attacks
- Account takeovers
- Man-in-the-middle attacks
- Fake websites/storefronts
- Fraudulent transactions/credit cards
- Coupon/promotion abuse
- Returns/damage fraud

Areas seen as particularly vulnerable to AI-enabled fraud

Automated phishing	82%
Synthetic Identity Creation	69%
Deepfake social engineering	69%
Payment/card fraud	62%
Refund/chargeback abuse	41%
Loyalty program/rewards	36%
Order manipulation	23%
Price manipulation	15%
Internal fraud	15%
Other	5%

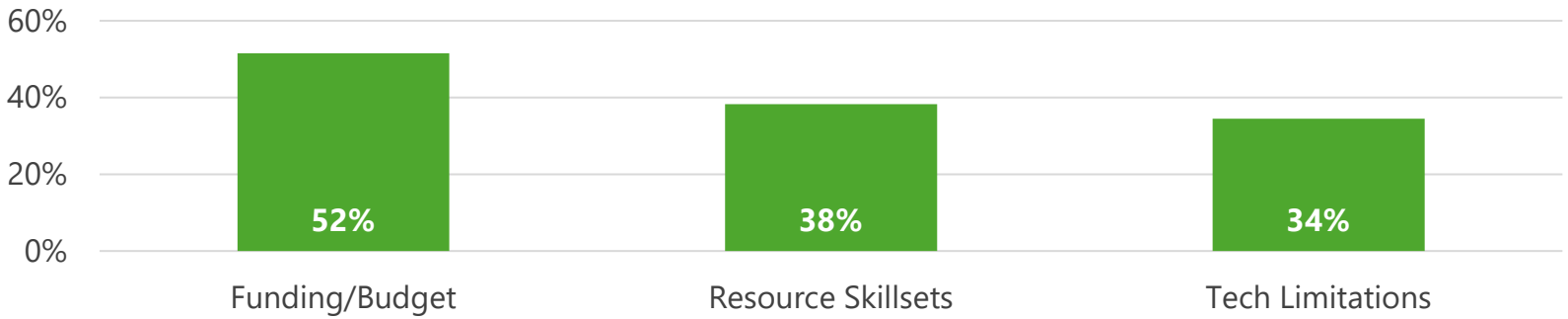
Expected increase in volume of agentic AI-enabled attacks in the next 12 months



95%

of merchants are planning to adapt their fraud strategy for agentic AI

Top barriers to implementing effective mitigation strategies against AI-enabled fraud



Respondents consistently emphasized keywords such as AI, fraud, automation, and agentic capabilities – signaling the areas expected to define the retail fraud landscape over the next 2-3 years.

The top emerging themes included:

- *"Greater difficulty distinguishing fraud from legitimate retail activity"*
- *"Escalating sophistication and volume of retail fraud attacks"*
- *"Expansion of scalable, low-cost AI-enabled fraud schemes"*
- *"Rapid evolution of fraud tactics through agentic AI and automation"*

Organizations that have updated their fraud strategy or implemented new controls to manage fraud enabled by AI

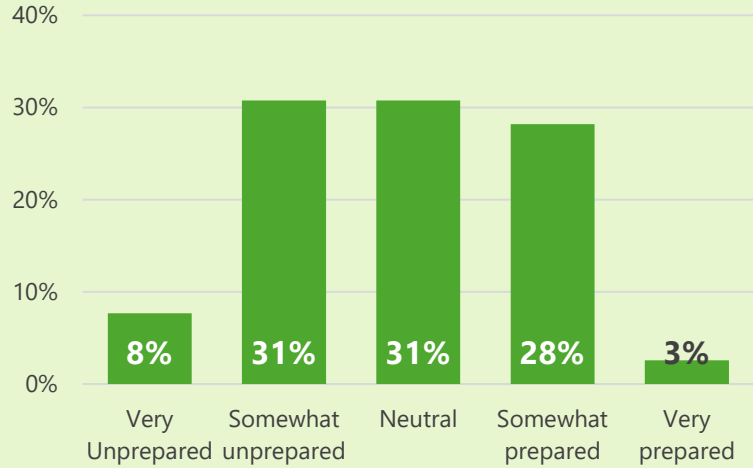
67% Yes

33% No

If replied 'Yes' to updating fraud strategy or implementing new controls, what have they worked on?

- Know Your Agent and risk models
- Penetration testing
- Multilevel authentication
- Adoption of industry best-practices
- Development of internal tool/procedures
- Controls focusing on AI for internal audit programs
- AI detection tools (e.g., adaptive AI, behavioral analytics, real-time threat orchestration)
- Inclusion of data use for AI in contracting language
- Reduction of human involvement for making fraud decisions
- Fortification of email and mobile security

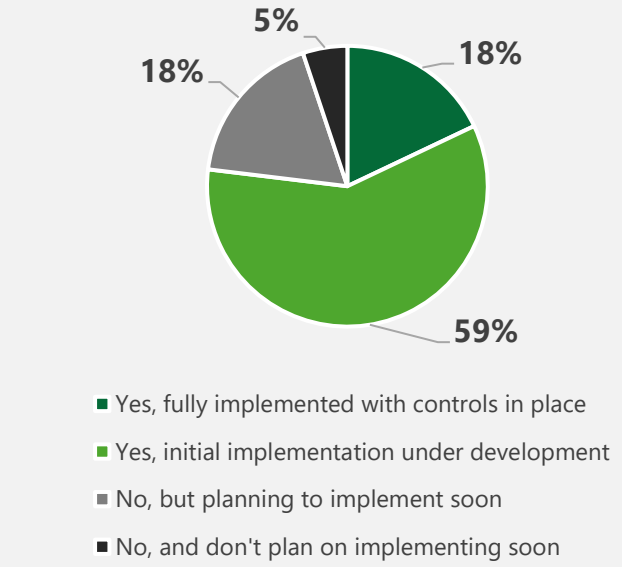
Merchant preparedness to handle AI-enabled fraud for the future



Mitigation strategies expected to be most effective against AI-enabled fraud

Industry-wide measures seen as most-needed to address AI-enabled fraud

Merchants currently using or considering using agentic AI in customer-facing channels



1. Deloitte estimate in "The future of commerce in an agentic world: How agentic AI will reshape commerce and what payment networks must do next", 2025.
2. Insight from Riskified proprietary data on LLM-referred traffic, transactions, and associated fraud, 2025.
3. Insight from Riskified proprietary data in "Global Study: 73% of Shoppers Using AI in Shopping Journey - But Merchants Face New Agentic Commerce Risks", 2025.
4. Insight from Riskified proprietary data in "Riskified Champions Fraud Prevention as a Leading Partner of International Fraud Awareness Week 2025", 2025.
5. Insight from HUMAN Security proprietary data in "Examining AI Agent Traffic: Powering the Shift to Agentic Commerce", 2025.

Deloitte.

www.deloitte.ca

About Deloitte

Deloitte provides audit and assurance, consulting, financial advisory, risk advisory, tax, and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and service to address clients' most complex business challenges. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited. Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Our global Purpose is making an impact that matters. At Deloitte Canada, that translates into building a better future by accelerating and expanding access to knowledge. We believe we can achieve this Purpose by living our shared values to lead the way, serve with integrity, take care of each other, foster inclusion, and collaborate for measurable impact.