EBOOK

Retail Identity & Metrics Mind Map

How identity decisions drive revenue, loyalty, and security

strivacity

Identity is where revenue is quietly lost

Identity sits in front of every high-value interaction: account creation, sign in, checkout, loyalty, and personalization. When identity creates friction, shoppers abandon. When it fails to protect, fraud follows. And when it buckles under peak traffic, the losses happen in the moments that matter most.

Yet identity remains one of the least measured parts of the retail stack. Most retailers have optimized checkout. Few have optimized the identity moments that happen before shoppers can pay or the infrastructure that needs to hold up when Black Friday, a flash sale, or seasonal surge hits.

For online retail businesses, this guide helps your security, digital, and product teams answer four critical questions:

What business outcomes can identity improve?

Which metrics expose the impact of identity on revenue, including mobile and at peak?

Which strategies will move those metrics?

How do teams align around an identity model that works for your business?

Retailers need an identity map

Retail identity is owned by multiple teams but rarely measured as a single system.

- Security focuses on **fraud**
- Digital focuses on **conversion**
- Product focuses on **speed**
- Marketing focuses on **engagement**
- Engineering focuses on **uptime**

The result is fragmented decisions, missed revenue, and no shared model for what “good” looks like. An identity map connects identity decisions to business outcomes like conversion, fraud reduction, loyalty, performance, and speed. It gives teams a shared model to prioritize and measure what matters.

Start with the outcomes your business already measures

Before diving into tactics, anchor your overall strategy to three outcomes that mean the most to leadership:

1. Reduce costs. Stemming fraud losses, support costs, identity-related engineering overhead, and the operational burden of disconnected tools protects revenue.

2. Grow the number of customers. Removing friction from account creation, sign in, and checkout directly improves conversion.

3. Increase revenue per customer. Strengthening loyalty, repeat purchases, recognition, and personalization across channels drives growth and long-term stability.

How identity impacts core retail KPIs

Identity directly impacts the metrics that retail leaders are accountable for:

	Retail KPI	How identity impacts it
1	**Conversion rate**	Account creation and sign in experience, account recovery, checkout completion
2	**Revenue per session**	Session continuity and customer recognition across channels
3	**Average order value (AOV)**	Personalization, saved preferences, and loyalty recognition
4	**Customer acquisition cost (CAC)**	Guest vs known conversion rates
5	**Customer lifetime value (CLV)**	Loyalty participation, repeat access, omnichannel engagement
6	**Account takeover (ATO) rate**	Preventing credential stuffing, phishing, social engineering, chargebacks, loyalty fraud

The retail identity metrics mind map

BETTER RETAIL IDENTITY IMPROVES FINANCIAL PERFORMANCE ACROSS FIVE OUTCOME AREAS:

1	2	3	4	5
Convert more shoppers	Protect every account	Build loyalty through trusted personalization	Increase agility and lower total cost of ownership	Prepare for AI-driven commerce
Jump to section >	Jump to section >	Jump to section >	Jump to section >	Jump to section >

Retailers often think of conversion as happening at product or checkout.
In reality, it's the outcome of a journey with multiple identity-driven steps:

Drop-off at any step due to friction reduces conversion.

The retail identity metrics mind map

CONVERT MORE SHOPPERS

- Optimize identity for peak traffic
- Remove friction for returning customers
- Reduce account creation abandonment
- Support guest checkout without losing long-term value

PROTECT EVERY ACCOUNT

- Prevent fake accounts at registration
- Continuously tune for peak periods
- Protect the front door and stop credential-based attacks
- Secure account recovery as a high-risk flow
- Protect loyalty as stored value

PREPARE FOR AI-DRIVEN COMMERCE

- Make authority explicit
- Maintain full auditability from day one
- Treat AI agents as identities, not tools
- Apply adaptive controls to agent behavior

BUILD LOYALTY THROUGH TRUSTED PERSONALIZATION

- Make recognition effortless across channels
- Build trust before personalization
- Prioritize trusted returning-user experiences
- Increase known customers over time

INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP

- Standardize before scaling
- Treat identity like a conversion funnel
- Remove engineering from routine changes
- Reduce complexity before reducing spend

Visible Simplicity. Invisible Sophistication.

The best retail identity experiences feel effortless while doing far more behind the scenes than the customer ever sees. Aim for visible simplicity with invisible sophistication.

	What customers see	What effective identity does
1	**Easy account creation**	Progressive profiling, social sign in, identity verification, bot detection, and fraud checks at registration
2	**Instant sign in on any device**	Passkeys, passwordless, social sign in, device recognition, breached password detection, risk-based authentication
3	**Frictionless checkout**	Session continuity and adaptive access controls, step-up only when risk is detected
4	**Personalized interactions**	Unified identity profiles, progressive profiling, consent and preference management
5	**No account lockouts**	Self-service account recovery, adaptive authentication, identity verification
6	**Recognized across every channel**	Centralized identity orchestration, account linking
7	**Safe but invisible security**	Bot detection, impossible travel detection, anomaly detection, behavioral analytics, API protection

Identity performance benchmarks

Retailers often track checkout performance, but many of the biggest conversion gaps are driven by identity friction, not pricing or product. Before teams decide what to fix first, they need a clear view of what strong identity performance actually looks like. These benchmarks provide directional ranges to help retailers identify where performance is strong and where identity is negatively impacting revenue.

	Metric	Good	Best-in-class	Primary identity-related driver
1	**Cart abandonment rate**	60–75%	<55%	Sign in friction
2	**Checkout completion rate**	25–40%	45–60%	Identity flow experience
3	**Sign in success rate**	>90%	>95%	Authentication experience
4	**Password reset success**	70–85%	90%+	Account recovery experience
5	**False positive rate**	5–10%	<3%	Fraud policy tuning
6	**Guest to account conversion**	20-40%	50%+	Post-purchase identity strategy
7	**Mobile sign in success rate**	> 85%	> 92%	Mobile-optimized authentication flows
8	**Omnichannel recognition rate**	40-60%	70%+	Unified identity profile, account linking

Source: Aggregated from industry research by Baymard Institute, Statista, Salesforce, Adobe, Stripe, MRC, and FIDO Alliance. Benchmarks represent directional ranges and vary by retailer and maturity.

These are not isolated metrics. They are signals that reveal how identity is performing at the most critical moments in the customer journey.

Low sign in success:	High password-reset friction:	High false positives:	Low guest conversion:	Low mobile sign in success:	Low omnichannel recognition:
returning customers cannot complete purchase	abandoned carts from known users	legitimate customers blocked at checkout	missed long-term customer value	abandoned sessions on the highest-traffic channel	loyalty that erodes every time a customer switches channel

In many retail environments, **30–50 percent of cart abandonment is tied to identity-related friction**, including authentication failures, recovery issues, and overly aggressive fraud controls. Even small improvements in sign in success, recovery, or false positive rates can translate directly into millions in recovered revenue for high-volume retailers.

Where to start

Most retailers do not need to start by measuring everything. They need to start with the metrics that expose the biggest leaks and highest revenue impact.

Start with the metrics that answer three questions:

- Where is identity creating revenue loss?
- Where is security creating unnecessary friction?
- Where is customer trust driving long-term value?

This starter set helps prioritize the highest impact metrics first before building a broader identity operating model.

Priority	Metric set	Why start here
1	**Cart abandonment, sign in performance, account creation performance**	Exposes where identity friction is hurting revenue most directly
2	**Verification outcomes, suspicious and blocked sessions, recovery requests**	Shows whether security controls are protecting trust without blocking customers
3	**Account engagement, known vs anonymous rate, consent opt-in**	Connects identity quality to long-term customer value
4	**Time to launch a journey, identity-related support tickets, number of tools/vendors**	Exposes the cost of identity complexity
5	**Agent verification, delegation, auditability**	Builds readiness for AI-driven commerce

Turning identity into measurable outcomes

To transform identity into a lever for growth, retailers must examine five key business drivers that hinge on identity performance:

CONVERSION

PROTECTION

LOYALTY

AGILITY

AI READINESS

Understanding each one starts by identifying:

- the business problem retailers need to solve
- the priority actions that improve outcomes
- the metrics that show whether those actions are working

The retail identity metrics mind map

CONVERT MORE SHOPPERS

- Remove friction for returning customers
- Optimize identity for peak traffic
- Reduce account creation abandonment
- Support guest checkout without losing long-term value

PROTECT EVERY ACCOUNT

- Prevent fake accounts at registration
- Continuously tune for peak periods
- Protect the front door and stop credential-based attacks
- Secure account recovery as a high-risk flow
- Protect loyalty as stored value

PREPARE FOR AI-DRIVEN COMMERCE

- Make authority explicit
- Maintain full auditability from day one
- Treat AI agents as identities, not tools
- Apply adaptive controls to agent behavior

BUILD LOYALTY THROUGH TRUSTED PERSONALIZATION

- Make recognition effortless across channels
- Build trust before personalization
- Prioritize trusted returning-user experiences
- Increase known customers over time

INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP

- Standardize before scaling
- Treat identity like a conversion funnel
- Remove engineering from routine changes
- Reduce complexity before reducing spend

1. Convert more shoppers

Industry research from Baymard reveals that **average cart abandonment rates hover near 70 percent**, yet large-scale retailers can **recapture up to 35 percent of that lost conversion** by refining the checkout journey. Much of this revenue leakage is tied directly to identity friction during the critical moments of sign in, account creation, and recovery. This is echoed by the FIDO Alliance, whose 2025 data shows that **48 percent of shoppers have walked away from a purchase** simply because they forgot a password—a failure point that is magnified on mobile, where abandonment happens in seconds.

Two specific patterns accelerate these losses. First, **mobile sign in success rates typically lag 5 to 10 percentage points behind desktop performance**, creating a significant revenue gap that often goes unmeasured. Second, authentication and recovery friction tend to spike during peak traffic surges, precisely when infrastructure strain and overly aggressive fraud controls are most likely to block legitimate customers. The result is a system that often performs worst exactly when and where the business needs it to perform best.

Priority actions

1

Remove friction for returning customers

Use passkeys, passwordless sign in, remembered devices, and adaptive authentication to eliminate unnecessary sign in barriers, especially on mobile.

2

Reduce account creation abandonment

Use progressive profiling, social sign in, and streamlined registration flows to capture only what is needed upfront to reduce abandonment.

3

Optimize identity for peak traffic

Use scalable authentication infrastructure, adaptive fraud controls, and step-level visibility so identity performs best when traffic is highest.

4

Support guest checkout without losing long-term value

Enable post-purchase account conversion, identity linking, and saved preference capture to preserve long-term customer value.

Key metrics to track

	Metric	What it measures	Why it matters in retail	Formula / definition	Primary owners
1	**Account creation performance** (success, abandonment, duration)	Registration outcomes including successful registrations, abandonment rates, and average completion time	Reveals whether friction is limiting new customer acquisition and conversion	Successful registrations, abandonment rate, and median registration duration	Product, Security
2	**Registration preferences** (social, multifactor authentication (MFA), passwordless)	Registration methods customers choose, including social sign in, MFA enrollment, and passwordless options	Indicates which registration paths reduce friction and improve conversion rates	Registrations by method/ Total registrations	Product, Security
3	**Sign in performance** (success, failure reasons, abandonment)	Success rates, failure reasons, and abandonment during authentication flows	Shows whether returning customers can access accounts and checkout without friction	Successful, failed, and abandoned sign in attempts / Total sign in attempts	Product, Security
4	**Identity verification outcomes**	Successful, failed, and abandoned identity verification during account creation or checkout	Ensures trust while preventing fraud without disrupting legitimate customer conversion	Successful verifications / Total verification attempts	Security, Fraud
5	**Checkout completion rate**	Share of initiated checkouts that result in purchase	Direct revenue indicator tied to identity friction	Completed orders / Started checkouts	Ecommerce, Digital

The retail identity metrics mind map

PROTECT EVERY ACCOUNT

- Prevent fake accounts at registration
- Protect the front door and stop credential-based attacks
- Continuously tune for peak periods
- Secure account recovery as a high-risk flow
- Protect loyalty as stored value

CONVERT MORE SHOPPERS

- Optimize identity for peak traffic
- Remove friction for returning customers
- Reduce account creation abandonment
- Support guest checkout without losing long-term value

PREPARE FOR AI-DRIVEN COMMERCE

- Make authority explicit
- Maintain full auditability from day one
- Treat AI agents as identities, not tools
- Apply adaptive controls to agent behavior

BUILD LOYALTY THROUGH TRUSTED PERSONALIZATION

- Make recognition effortless across channels
- Build trust before personalization
- Prioritize trusted returning-user experiences
- Increase known customers over time

INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP

- Standardize before scaling
- Treat identity like a conversion funnel
- Remove engineering from routine changes
- Reduce complexity before reducing spend

2. Protect every account

Retail accounts are high-value targets. They hold personal data, saved payment methods, and stored value through loyalty programs. Attackers target these accounts because they can be monetized quickly and at scale. According to Verizon's 2025 Data Breach Investigations Report, **88 percent of attacks involve stolen credentials**. In retail, that makes credential theft the primary entry point for fraud.

Credential theft drives account takeover at scale

Most retail fraud begins before a customer ever reaches your site. Attackers use breached credentials from other services and automate login attempts through credential stuffing and password spraying. Because customers reuse passwords, a single breach elsewhere can unlock thousands of retail accounts. The highest-risk moments are sign in and account recovery. Sign in is targeted at scale with automated attacks, while account recovery is often exploited to bypass authentication controls altogether.

This becomes significantly harder to manage during peak periods. High volumes of legitimate traffic make attack patterns more difficult to distinguish, and fraud controls that work under normal conditions often overcorrect, blocking real customers at the worst possible time. That creates a direct tradeoff between security and conversion when retailers can least afford it.

Loyalty fraud is where stolen access is monetized

Once attackers gain access, they move quickly to extract value. Loyalty programs are one of the easiest and most profitable targets. Loyalty points act like currency. They can be redeemed, transferred, or resold, often with less scrutiny than payment methods.

Stage	What happens	Business impact
Account creation	**Fake or bot-driven accounts created to exploit promotions**	Increased acquisition cost and incentive abuse
Sign in	**Compromised credentials used for account takeover**	Unauthorized access to rewards and customer data
Redemption	**Fraudulent use of loyalty points or rewards**	Direct revenue loss and customer dissatisfaction

Priority actions

1

Protect the front door and stop credential-based attacks

Use bot detection, breached credential checks, and adaptive authentication at sign in to reduce account takeover.

2

Secure account recovery as a high-risk flow

Add identity verification and adaptive controls to prevent attackers from bypassing authentication through password reset.

3

Prevent fake accounts at registration

Stop promotion abuse early with bot detection and identity checks.

4

Protect loyalty as stored value

Apply step-up authentication and monitoring to high-risk actions such as redemption, transfers, and profile changes.

5

Continuously tune for peak periods

Use unified fraud signals and real-time insights to reduce false positives while maintaining protection when traffic spikes.

Key metrics to track

	Metric	What it measures	Why it matters in retail	Formula / definition	Primary owners
1	**Identity verification and fraud transactions**	Identity verification attempts, including success, failure and fraud outcomes	Prevents fake accounts, synthetic identities, and fraudulent account creation before abuse begins	Verification outcomes + fraud transactions / Total verification attempts	Security, Fraud
2	**Step-up authentication outcomes**	Authentication events that trigger additional verification and the reasons behind them	Indicates whether adaptive security is protecting accounts without creating unnecessary friction	Step-up events and reasons / Total authentication events	Security
3	**Blocked sessions by reason**	Suspicious sign in attempts by origin such as bots, IP risk, or improbable travel	Helps identify fraud patterns while reducing false positives that impact conversion	Blocked sessions by reason / Total blocked sessions	Security
4	**Sign in attempts with disabled accounts**	Attempts to access locked, suspended, or disabled accounts	Strong signal of credential stuffing, fraud attempts, or repeated account takeover behavior	Disabled account sign in attempts / Total sign in attempts	Security, Fraud
5	**Account recovery requests**	Password reset requests, failed sign ins, and lockouts	Highlights compromised credentials, customer friction, and recovery abuse risks	(Failed sign ins + password reset requests + account lockouts) / Total sign in attempts	Security, Support

The retail identity metrics mind map

CONVERT MORE SHOPPERS

- Optimize identity for peak traffic
- Remove friction for returning customers
- Reduce account creation abandonment
- Support guest checkout without losing long-term value

PROTECT EVERY ACCOUNT

- Prevent fake accounts at registration
- Continuously tune for peak periods
- Protect the front door and stop credential-based attacks
- Secure account recovery as a high-risk flow
- Protect loyalty as stored value

PREPARE FOR AI-DRIVEN COMMERCE

- Make authority explicit
- Maintain full auditability from day one
- Treat AI agents as identities, not tools
- Apply adaptive controls to agent behavior

INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP

- Standardize before scaling
- Treat identity like a conversion funnel
- Remove engineering from routine changes
- Reduce complexity before reducing spend

BUILD LOYALTY THROUGH TRUSTED PERSONALIZATION

- Make recognition effortless across channels
- Build trust before personalization
- Prioritize trusted returning-user experiences
- Increase known customers over time

3. Build loyalty through trusted personalization

Retailers grow loyalty when customers feel known, recognized, and remembered across every interaction. Known customers are significantly more valuable than anonymous ones. McKinsey & Company found that **companies that excel at personalization generate 40 percent more revenue** from those activities than average players, driven by repeat purchases, higher engagement, and improved retention.

But personalization only works when identity creates trust and continuity. Customers expect order history, saved preferences, personalized offers, and loyalty benefits to follow them across web, mobile, app, store, and service interactions. They expect brands to recognize them without forcing repeated sign ins, unnecessary friction, or disconnected experiences across channels.

The goal is not to collect more data. It is to create more relevant, trusted customer experiences that make customers return more often and generate greater lifetime value.

Priority actions

1

Make recognition effortless across channels

Use unified identity profiles, account linking, and omnichannel orchestration so customers are recognized consistently across every channel.

2

Prioritize trusted returning-user experiences

Use remembered devices, passkeys, passwordless access, and session continuity to reduce friction for returning customers.

3

Build trust before personalization

Use centralized consent management, preference controls, and self-service profile management so personalization is based on trust and transparency.

4

Increase known customers over time

Use progressive profiling and low-friction authentication to enrich customer profiles over time without creating registration barriers.

Key metrics to track

	Metric	What it measures	Why it matters in retail	Formula / definition	Primary owners
1	**Active account rate**	The number of active customer accounts compared to total registered accounts over a given period	Shows whether customers are returning and maintaining ongoing engagement with the brand	Active accounts / Total accounts	Product, Digital
2	**Known vs anonymous customer rate**	Share of traffic tied to a known identity	Indicates how well identity supports personalization and retention	Known active users / Total active users	Digital, CRM
3	**Omnichannel recognition rate**	Customers recognized consistently across web, mobile, app, and in-store	Measures trust and readiness for personalized engagement	Cross-channel recognized / Total sessions	Digital
4	**Consent opt-in rate**	Share of customers granting optional consent	Measures trust and readiness for personalized engagement	Customers opted in / Customers prompted	Marketing, Compliance
5	**Sign in preferences**	Sign in methods customers choose, including social sign in, MFA, and passwordless options	Indicates which sign in paths reduce friction and improve repeat purchases	Sign ins by method / Total sign ins	Product, Security


The retail identity metrics mind map
CONVERT MORE SHOPPERS
Optimize identity for peak traffic
Remove friction for returning customers
Reduce account creation abandonment
Support guest checkout without losing long-term value
PROTECT EVERY ACCOUNT
Prevent fake accounts at registration
Continuously tune for peak periods
Protect the front door and stop credential-based attacks
Secure account recovery as a high-risk flow
Protect loyalty as stored value
PREPARE FOR AI-DRIVEN COMMERCE
Make authority explicit
Maintain full auditability from day one
Treat AI agents as identities, not tools
Apply adaptive controls to agent behavior
BUILD LOYALTY THROUGH TRUSTED PERSONALIZATION
Make recognition effortless across channels
Build trust before personalization
Prioritize trusted returning-user experiences
Increase known customers over time
Standardize before scaling
Treat identity like a conversion funnel
INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP
Remove engineering from routine changes
Reduce complexity before reducing spend

4. Increase agility and lower total cost of ownership

Retailers need identity that moves at the speed of the business. When every sign in page change, consent update, or new brand launch requires engineering time, identity becomes a bottleneck. Deloitte found that 44 percent of retail executives say legacy systems are slowing innovation. The Retail & Hospitality ISAC 2026 CISO Benchmark Report adds that **70 percent report IT prioritization challenges and 68 percent cite budget constraints as major execution barriers**.

Cost and speed problems compound at peak. Shared multi-tenant infrastructure can introduce performance variability when traffic spikes. Disconnected tools mean no unified view when something breaks during a revenue window. And the engineering effort required to debug a fragmented identity stack during a live event scales costs at the worst possible time.

Priority actions

1

Reduce complexity before reducing spend

Fewer systems create faster execution, lower support costs, and better visibility across identity journeys.

2

Remove engineering from routine changes

Identity should move at the speed of the business, not the speed of backlog prioritization.

3

Treat identity like a conversion funnel

Use testing, abandonment, and failure data to continuously improve performance.

4

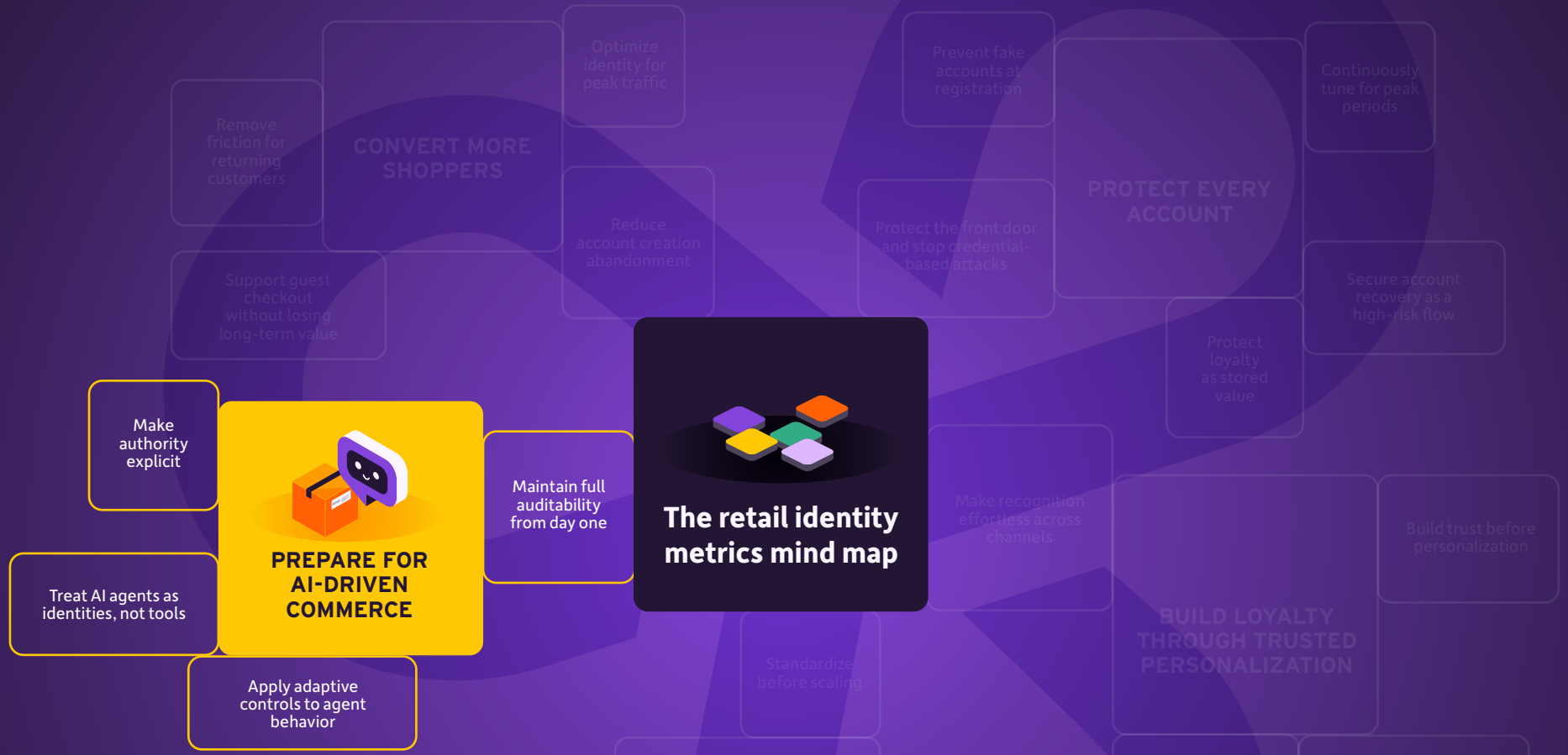
Standardize before scaling

Consistent identity flows across brands and applications reduce cost, duplication, and operational risk.

INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP

Key metrics to track

	Metric	What it measures	Why it matters in retail	Formula / definition	Primary owners
1	**Time to launch a new journey or change a policy**	Days or weeks needed to launch or update registration, sign in, consent changes	Flags the potential for missing windows during peak seasons	Average time from request to production launch	Product, Engineering
2	**Journey optimization**	Side-by-side visibility into customer journey flows	Unlocks a data-driven evaluation of flow changes to optimize account creation and conversion	Baseline / variant	Product, Digital
3	**Number of identity tools/ vendors**	Count of separate systems used across identity functions	Highlights potential for higher cost and complexity	Total tools in active identity stack	IT, Procurement
4	**Identity-related support tickets**	Volume of customer support tied to access or account issues	Signals friction and cost when volume is high	Total identity-related support tickets per period	Support, Product
5	**Cost per active identity**	Operational and licensing cost per active user or transaction	Helps quantify total cost of ownership	Total identity cost / Active identities or monthly active users	Finance, IT


The retail identity metrics mind map
PREPARE FOR AI-DRIVEN COMMERCE
Make authority explicit
Treat AI agents as identities, not tools
Apply adaptive controls to agent behavior
Maintain full auditability from day one
CONVERT MORE SHOPPERS
Optimize identity for peak traffic
Remove friction for returning customers
Reduce account creation abandonment
Support guest checkout without losing long-term value
PROTECT EVERY ACCOUNT
Prevent fake accounts at registration
Continuously tune for peak periods
Protect the front door and stop credential-based attacks
Secure account recovery as a high-risk flow
Protect loyalty as stored value
BUILD LOYALTY THROUGH TRUSTED PERSONALIZATION
Make recognition effortless across channels
Build trust before personalization
Prioritize trusted returning-user experiences
Increase known customers over time
INCREASE AGILITY AND LOWER TOTAL COST OF OWNERSHIP
Standardize before scaling
Treat identity like a conversion funnel
Remove engineering from routine changes
Reduce complexity before reducing spend

5. Prepare for AI-driven commerce

Retail identity is expanding beyond human users. Bain & Company estimates that **US agentic commerce could reach $300– $500 billion by 2030, or roughly 15–25 percent of ecommerce**. As AI-driven commerce grows, the challenge is not adoption, but control. Retailers must verify AI agents, govern what they can do, and maintain full visibility into every action.

This transition has already begun. AI shopping assistants are helping customers discover and purchase products. Automated agents are interacting with accounts and loyalty systems. AI-driven service experiences are modifying customer data. Most retailers are not yet measuring any of it.

Priority actions

1

Treat AI agents as identities, not tools

If an agent can act like a person, it must be verified, governed, and monitored like one.

2

Make authority explicit

Every agent action should be tied to verified delegation, scope, and customer consent.

3

Apply adaptive controls to agent behavior

High-risk actions should trigger step-up verification or human approval.

4

Maintain full auditability from day one

Trust, compliance, and dispute resolution depend on proving who did what, when, and why.

For most retailers, this represents the forward edge of identity maturity.

If you are still working on sign in success rates and mobile conversion, start there. Apply these tips when agentic commerce becomes part of your roadmap.

Key metrics to track

	Metric	What it measures	Why it matters in retail	Formula / definition	Primary owners
1	**Agent identity verification rate**	% of agents and associated humans that are identity-verified (Know Your Agent)	Ensures only trusted agents interact with customer accounts and systems	Verified agents / Total registered agents	Security, Fraud
2	**Delegated authorization rate**	% of agent actions performed with valid, scoped delegation	Ensures agents act only within approved authority	Authorized agent actions / Total agent actions	Security, Governance
3	**Unauthorized agent action rate**	Actions attempted without valid delegation or authority	Identifies control gaps and potential abuse	Unauthorized agent actions / Total agent actions	Security
4	**Consent-backed agent action rate**	% of agent actions tied to valid customer consent	Confirms agents operate under approved permissions and terms	Consent-backed actions / Total eligible agent actions	Compliance, Product
5	**Agent auditability rate**	% of agent actions with full traceability (who, what, when, why)	Critical for trust, dispute resolution, and compliance	Fully auditable agent actions / Total agent actions	Security, Compliance

What this requires from modern retail identity

Retailers do not need more identity tools. They need a simpler, unified way to manage identity across the customer journey. Today, identity is often fragmented across registration, authentication, fraud, consent, and customer data systems.

To support both growth and protection, retailers must:

1

Connect the full identity lifecycle.

From registration to sign in, loyalty, and recovery, identity cannot be fragmented across systems. Gaps create friction for customers and blind spots for the business.

2

Balance conversion and protection in real time.

Security should adapt to risk without disrupting legitimate customers. The same system that protects accounts should also support smooth sign in and checkout.

3

Deliver consistent performance at scale.

Identity infrastructure must hold up during peak demand, not just average traffic. Single-instance architecture, pre-tuned fraud thresholds, and load-tested recovery flows are essential for high-volume retailers.

4

Win on mobile without a separate strategy.

Mobile should not require a different identity stack. A unified system should support native mobile experiences such as passkeys, biometrics, and push authentication for every channel – without custom engineering.

5

Provide visibility into identity performance.

Teams need a clear view of where identity creates friction, where it reduces risk, and how it impacts business outcomes across every channel and traffic condition.

6

Enable speed without heavy engineering.

Identity should move at the pace of the business, allowing teams to launch, adapt, and improve without long development cycles.

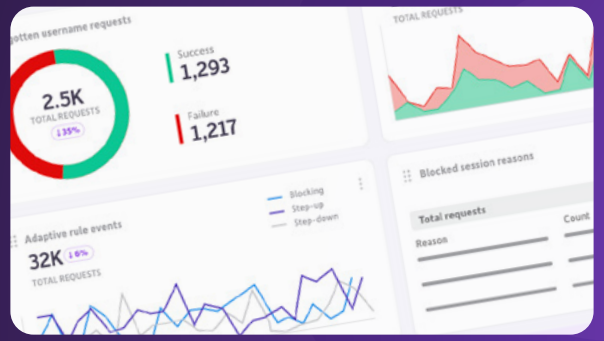
Retail identity is now a growth metric

Every registration step, sign in prompt, password reset, consent interaction, and fraud check affects whether a shopper converts, whether they trust your brand, and whether they come back.

The retailers that win will measure identity the same way they measure checkout, loyalty, and customer experience: as part of the revenue engine. That means understanding where identity creates friction, where it reduces risk, and where it helps build stronger customer relationships over time.

Want to learn more?

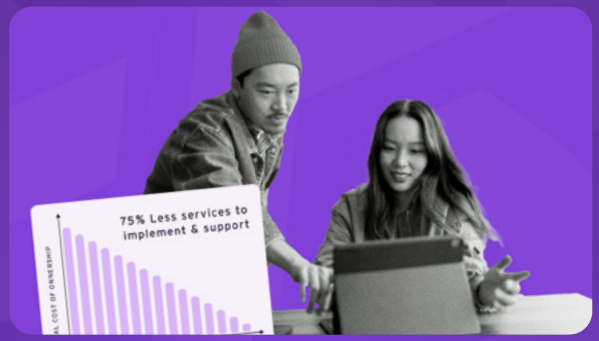
Take the next step toward improving your identity journeys and measuring where identity impacts revenue, loyalty, and customer trust.



Explore customer insights

See how identity data helps uncover friction points, reduce abandonment, and improve sign in, sign-up, and recovery performance across the customer journey.

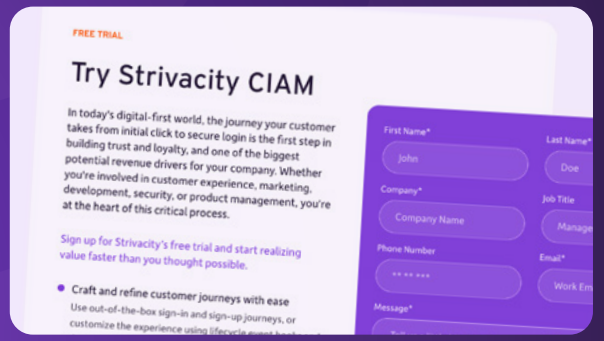
https://www.strivacity.com/capabilities/customer-insights ↗



Request a customer journey assessment

Engage our team to review your current identity experience, identify quick wins, and uncover longer term opportunities to improve conversion and reduce operational friction.

https://www.strivacity.com/why-strivacity/problems-we-solve/customer-journey-analysis ↗



Upgrade your CIAM provider

See how leading brands are moving away from legacy identity platforms to reduce complexity, improve performance, and lower total cost of ownership.

https://www.strivacity.com/problems-we-solve/replace-your-ciam-solution ↗

Retail Identity & Metrics Mind Map

The ultimate guide to measuring how identity decisions drive revenue, loyalty, and security

ABOUT US

Strivacity is The AI Identity Company that helps brands deliver trusted digital experiences by managing agentic, customer, and partner identities in a single product.

It brings identity orchestration, account opening, sign in, consent management, and fraud prevention together to reduce friction, improve conversion, and give business and security teams clear visibility into where identity drives or blocks growth.

Built on a single-instance SaaS architecture with data residency by design, Strivacity helps organizations modernize customer identity while preparing for the agentic AI era.

205 Van Buren Street
Suite 120
Herndon, VA 20170

+1 844 782 5486 strivacity.com