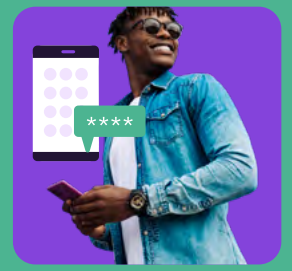
EBOOK

Customer Identity Metrics Mind Map for Financial Services

The ultimate guide to measuring customer identity journeys that drive growth, reduce risk, and improve compliance



strivacity

The five business outcomes that matter most

When you're talking to executives in banking, insurance, or wealth management, it pays to lead with what matters most in the boardroom: business outcomes.

Whether you're modernizing authentication, meeting evolving compliance standards, or improving digital onboarding, leadership wants to know one thing: How does this drive growth, reduce risk, and improve compliance?

THAT'S WHY THIS MIND MAP TIES EVERY STRATEGY AND METRIC BACK TO FIVE CORE LEVERS:

1	2	3	4	5
Lower operational costs	**Prevent fraud**	**Increase account opening rates**	**Grow revenue per customer**	**Meet compliance requirements**
Jump to section >	Jump to section >	Jump to section >	Jump to section >	Jump to section >

Your identity platform influences all five. These are the outcomes that get buy-in from the board and they all depend on how smooth, secure, and scalable your sign-in experience is.


LOWER OPERATIONAL COSTS
Reduce support call volume & password resets
Eliminate duplicate tools and redundant licenses)
Reduce IT maintenance & compliance overhead
PREVENT FRAUD
Block high-risk access
automate fraud response
Detect threats early
Strengthen identity verification
INCREASE ACCOUNT OPENING RATES
Speed transactions
Simplify account opening
Automate Identity verification & KYC checks
Increase referral acquisitions
Modern identity, measurable results
Personalize engagement
GROW REVENUE PER CUSTOMER
Enable self-service
Increase repeat visits
Reduce account abandonment
Increase loyalty & referral programs
Build accessible experiences
MEET COMPLIANCE REQUIREMENTS
Ensure strong authentication
Centralize audit trails
Increase repeat visits
Enforce Data residency & sovereignty rules

Why a mind map?

Improving customer journeys in financial services is more than just good UX. It's a strategic balancing act between growth, compliance, and security. With teams across digital banking, fraud, marketing, compliance, and IT all focused on different KPIs, it's easy to lose the bigger picture.

This mind map connects the dots. Whether you're reducing account abandonment, cutting fraud, or speeding up onboarding, you'll see how identity strategies tie directly to business outcomes.

How to use the mind map

This isn't just a list of metrics; it's a blueprint for aligning your identity strategy to business impact. In financial services, alignment across functions is everything. This map helps you connect the dots between experience, security, compliance, and outcomes your leadership cares about.

Here's how to use it:

Start with a business goal

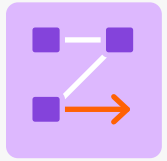
Whether you're trying to reduce fraud losses or increase digital conversion, begin with a clear outcome. Then use the map to identify the metrics and CIAM capabilities that support it.

Pick a metric, work backward

Focused on a specific KPI like MFA adoption or KYC drop-off? Find it in the map and trace it back to the identity tactics that drive it.

Align cross-functional teams

Use the mind map to get security, digital, marketing, and compliance on the same page. It clarifies how their goals connect to identity and how identity connects to growth, risk, and retention.

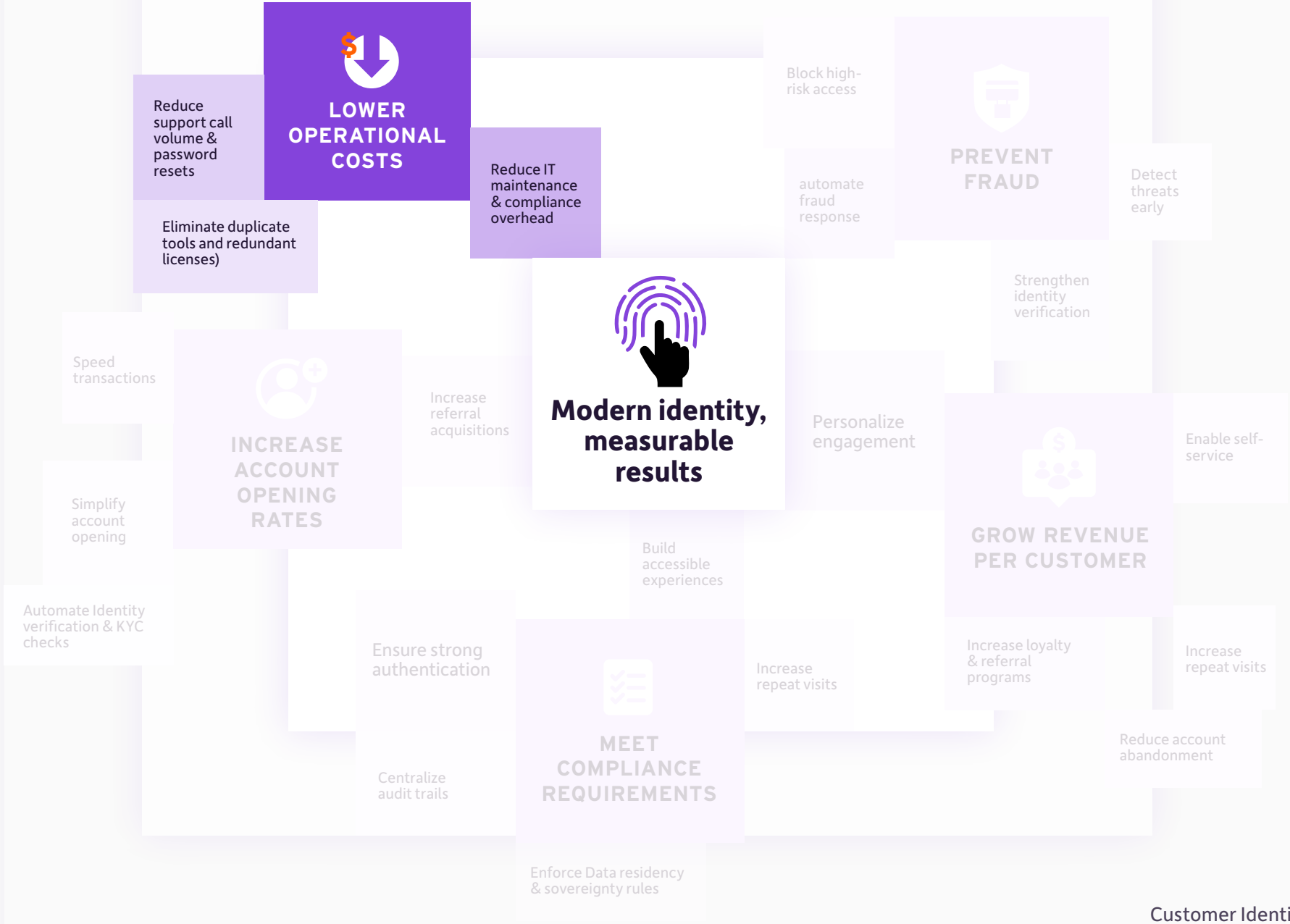


Frame board-level conversations

When stakeholders ask "How does identity improve business performance?" this framework shows the path from authentication to ROI.

1 Lower operational costs

Identity friction doesn't just frustrate customers, it drains resources. From overloaded call centers to maintenance-heavy legacy systems, inefficient sign-in experiences quietly rack up costs across your organization. The good news? Optimizing CIAM reduces operational burden while improving customer satisfaction.


LOWER OPERATIONAL COSTS
Reduce support call volume & password resets
Eliminate duplicate tools and redundant licenses)
Reduce IT maintenance & compliance overhead
Modern identity, measurable results
PREVENT FRAUD
Block high-risk access
automate fraud response
Detect threats early
Strengthen identity verification
INCREASE ACCOUNT OPENING RATES
Speed transactions
Simplify account opening
Automate Identity verification & KYC checks
Increase referral acquisitions
Personalize engagement
GROW REVENUE PER CUSTOMER
Enable self-service
Build accessible experiences
Increase repeat visits
Increase loyalty & referral programs
Reduce account abandonment
MEET COMPLIANCE REQUIREMENTS
Ensure strong authentication
Centralize audit trails
Enforce Data residency & sovereignty rules

Strategies to reduce the cost of sign-up and sign-in journeys

1

Lower support call volume and password resets

Sign-in issues like forgotten passwords and lockouts are a top driver of support calls. By adopting more intuitive authentication methods like passkeys, biometrics, or adaptive MFA, you reduce friction and free up your support team.

Metric to track:

% of total support volume tied to sign-in issues

2

Reduce it maintenance and compliance overhead

Legacy identity systems require custom integrations, manual updates, and time-consuming audits. A modern CIAM platform streamlines maintenance, simplifies compliance with regulations like GDPR, GLBA, and PCI-DSS, and provides centralized logs for faster audit readiness.

Metric to track:

% reduction in hours spent on identity-related maintenance and audit preparation

3

Eliminate duplicate tools and redundant licenses

Most financial institutions have accumulated point solutions for MFA, fraud detection, and consent management. Consolidating into a unified CIAM platform cuts licensing and integration costs and simplifies procurement and administration.

Approach:

Map all tools tied to sign-in and calculate total cost of ownership per MAU

The bottom line:

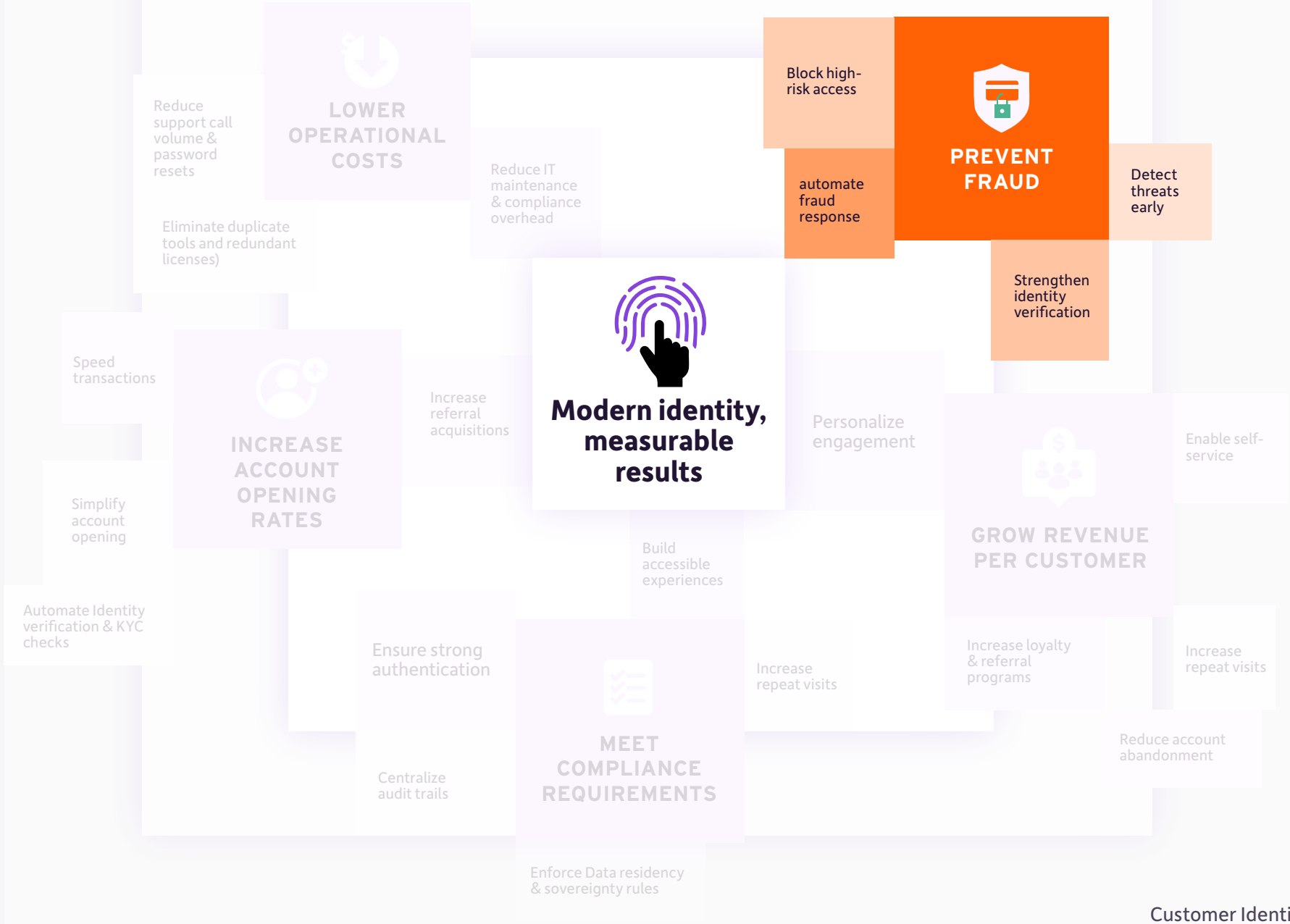
Modernizing your sign-in experience pays off on both sides of the ledger. It reduces the volume of operational headaches and cuts the time and money spent stitching solutions together. In a high-margin, high-risk industry like financial services, that's a strategic win.

See the table below for metrics and how to measure them.

	Metric	Why it matters	How CIAM supports	How to measure
1	**Cost of investigating online incidents**	Manual investigations slow down security response and drain team resources	Unified logging, session tracking, and real-time insights speed investigations	Time and labor cost per incident (from alert to resolution)
2	**Use of automation and identity context**	Reduces effort and shortens time to detect and resolve issues	Risk-based workflows, adaptive authentication, session blocking, audit-ready reports	% of support cases resolved without human intervention
3	**Self-service customer support**	Reduces support volume and empowers customers to solve login issues independently	Passwordless login, user-friendly account recovery and device based trust	# support calls; % password resets resolved without help desk involvement
4	**Software licensing costs**	Too many tools drive up per-user identity costs	Usage-based licensing and consolidated capabilities reduce overhead	Monthly active user (MAU) licensing cost
5	**Tooling redundancy**	Overlapping tools increase cost, complexity, and integration risks	Unified CIAM with built-in MFA, fraud, and consent management	# of duplicate tools for authentication, consent, fraud detection
6	**Reliance on 3rd party consulting**	Consulting services increase setup and ongoing maintenance costs	Built-in features reduce need for custom code or external integrations	Annual spend on CIAM consulting and customization
7	**Maintenance and support time**	Routine upkeep adds to engineering and IT workloads	CIAM vendor handles updates, patching, and scaling	Hours per week/month spent on CIAM system maintenance
8	**Engineering time for new features and changes**	CIAM custom work delays feature launches/ updates and drains internal resources	Low-code orchestration and reusable policies accelerate delivery	Hours/month spent on CIAM-related development or configuration
9	**Time spent on audit support**	Audits are time-consuming without centralized identity data and access logs	Out-of-the-box dashboards and centralized logging in one place	Hours/months required for audit preparation and response

2 Prevent fraud

In financial services, fraud prevention isn't just risk management, it's a competitive advantage. From account takeovers and credential stuffing to synthetic identity fraud at onboarding, the threats are evolving fast and getting more expensive. To stay ahead, financial institutions must proactively detect and stop fraud across the entire identity lifecycle, starting at sign-up and without compromising customer experience.


Modern identity, measurable results
PREVENT FRAUD
Block high-risk access
automate fraud response
Detect threats early
Strengthen identity verification
LOWER OPERATIONAL COSTS
Reduce support call volume & password resets
Eliminate duplicate tools and redundant licenses)
Reduce IT maintenance & compliance overhead
INCREASE ACCOUNT OPENING RATES
Speed transactions
Simplify account opening
Automate Identity verification & KYC checks
Increase referral acquisitions
Ensure strong authentication
Centralize audit trails
MEET COMPLIANCE REQUIREMENTS
Enforce Data residency & sovereignty rules
Build accessible experiences
Personalize engagement
GROW REVENUE PER CUSTOMER
Enable self-service
Increase loyalty & referral programs
Increase repeat visits
Reduce account abandonment

Strategies for reducing identity-related fraud

1

Detect threats early using behavioral signals

CIAM platforms use behavioral analytics including device posture and login patterns to detect anomalies before fraud occurs. Early detection reduces both direct losses and downstream investigation costs.

Metric to track:

Number of fraud attempts blocked before login success

2

Use adaptive authentication to block high-risk access

Instead of treating all customers the same, adaptive authentication dynamically adjusts based on real-time context like location, device, and behavior. High-risk attempts are challenged; trusted customers get a seamless experience.

Metric to track:

% of sign-ins flagged as high-risk vs. actual confirmed fraud rate

3

Strengthen identity verification at account creation

Fraud often starts at sign-up with stolen credentials or fake identities. Integrating identity verification tools (e.g., document scans, liveness checks, or data validation) helps stop fraud at the front door.

Metric to track:

% of fraudulent sign-up attempts blocked during account opening

4

Automate fraud response to reduce investigation time

CIAM platforms with built-in workflows and centralized logs help fraud and security teams respond faster. That means fewer manual investigations, lower recovery costs, and better protection for affected users.

Metric to track:

Average time to detect and respond to fraud incidents

5

Reduce false positives to protect good customers

Overly strict fraud rules can lock out or frustrate legitimate customers. CIAM helps fine-tune your risk engines so only suspicious activity gets flagged while trusted customers sail through.

Best practice:

Track false-positive rates and authentication-related abandonment

The bottom line:

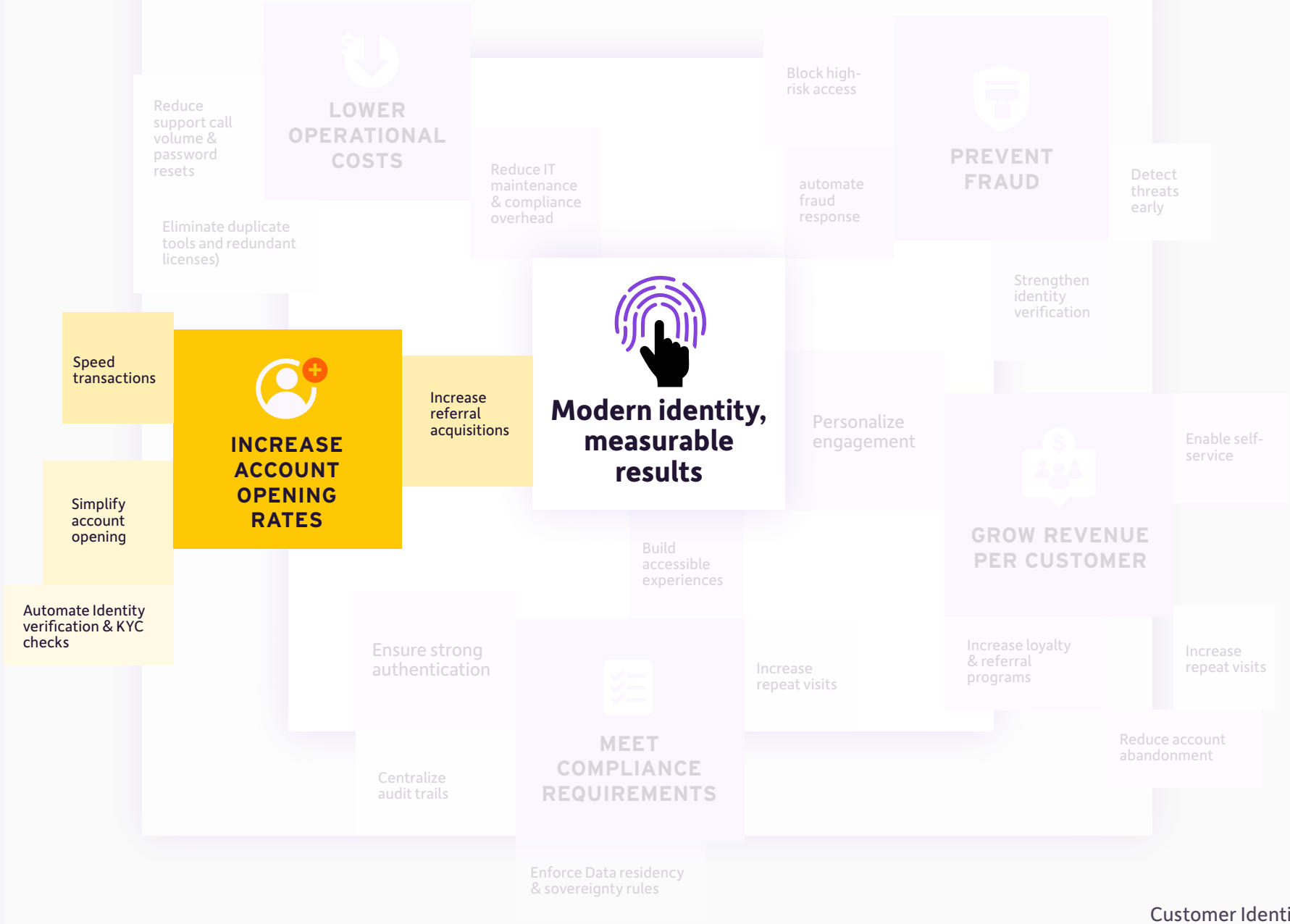
Preventing fraud is not just about stopping bad actors. It is about balancing trust, security, and experience. A modern CIAM approach gives you the tools to do all three. By covering both sign-up and sign-in journeys, financial services firms can stay ahead of evolving threats while reducing friction and fraud-related costs.

See the table below for metrics and how to measure them.

	Metric	Why it matters	How CIAM supports	How to measure
1	**% of fraudulent account creation attempts stopped at onboarding**	Stops fraud at the front door before accounts are abused	Real-time identity proofing, behavioral analytics, and verification insights	# of blocked sign-up attempts by threat
2	**Login failures**	High failure rates may indicate credential stuffing or account takeover attempts	Passkeys, Strong MFA, device recognition, breached credential checks, and login analytics dashboards	# of account takeovers and attempted takeovers per month $ impact per incident
3	**Use of automation and identity context**	Reduces effort and shortens time to detect and resolve fraud	Adaptive authentication, risk signals, session blocking, audit-ready reporting	% of fraud cases resolved without manual review
4	**Loyalty fraud attempts detected**	Loyalty fraud impacts brand trust and drives hidden financial losses	Behavior analytics and risk-based step-up authentication for suspicious redemptions	# of step-up challenges or blocked sessions
5	**Blocked sessions by reason**	Visibility into which threats are being stopped and why	Policy-based session blocking by geography, IP risk, device, or behavior	# blocked sessions, categorized by policy trigger
6	**Account lockouts**	High lockout rats can point to attack or friction issues	Smarter recovery flows and context-aware lockout prevention	# lockouts per week/month
7	**Password resets**	Spikes in resets may indicate poor UX or compromised accounts	Passwordless login, passkey support, and anomaly flagging	Password reset rate over time; Trends alongside failed login attempts

3 Increase account opening rates

Digital acquisition is only as strong as your account opening experience. If identity checks create too much friction, customers abandon. But streamlining account opening while staying compliant with KYC and AML doesn't have to be a trade-off. Smarter sign-up flows, personalized journeys, and real-time verification tools remove hurdles without compromising on security. This helps you turn more prospects into loyal customers.


LOWER OPERATIONAL COSTS
Reduce support call volume & password resets
Eliminate duplicate tools and redundant licenses)
Reduce IT maintenance & compliance overhead
Block high-risk access
automate fraud response
PREVENT FRAUD
Detect threats early
Strengthen identity verification
Speed transactions
Simplify account opening
Automate Identity verification & KYC checks
INCREASE ACCOUNT OPENING RATES
Increase referral acquisitions
Modern identity, measurable results
Personalize engagement
Enable self-service
GROW REVENUE PER CUSTOMER
Build accessible experiences
Ensure strong authentication
Increase repeat visits
Increase loyalty & referral programs
Increase repeat visits
Reduce account abandonment
MEET COMPLIANCE REQUIREMENTS
Centralize audit trails
Enforce Data residency & sovereignty rules

Strategies to turn more prospects into customers

1

Simplify the sign-up experience

Replace long forms and confusing flows with progressive profiling and saved-state onboarding. Let customers sign up using existing credentials (federated login, ID verification services) to reduce drop-off.

Metric to track:

Sign-up conversion rate and onboarding abandonment, A/B test account opening experiencessuccess

2

Automate identity verification and KYC checks

Manual reviews delay account opening and drive drop-off. Embed real-time verification using IDV tools that meet compliance standards (KYC, AML, NAIC), all without routing users to offline or high-friction steps.

Metric to track:

KYC pass rate, time to verify, drop-off during verification

3

Speed up time to first transaction

Don't stop at "account created." Use post-login call-to-actions and personalized landing pages to guide customers directly to their first value-driving action like funding an account or starting a quote.

Metric to track:

Average time to first transaction

4

Reduce friction for return visits

Make reauthentication seamless. Remember trusted devices, offer passwordless options, and adapt MFA based on user context so returning customers can pick up right where they left off.

Metric to track:

Returning customer sign-in success rate

5

Increase acquisition through referrals

Referral programs drive acquisition but only if customers can access and share them easily. Embed referral prompts securely into the account opening flow with built-in fraud protections and compliance controls.

Metric to track:

Invite-to-sign-up referral rate

The bottom line:

Simplifying account opening isn't just about aesthetics. It directly improves acquisition ROI, speeds up revenue, and reduces the chance that fraud or compliance checks block the path to customer growth.

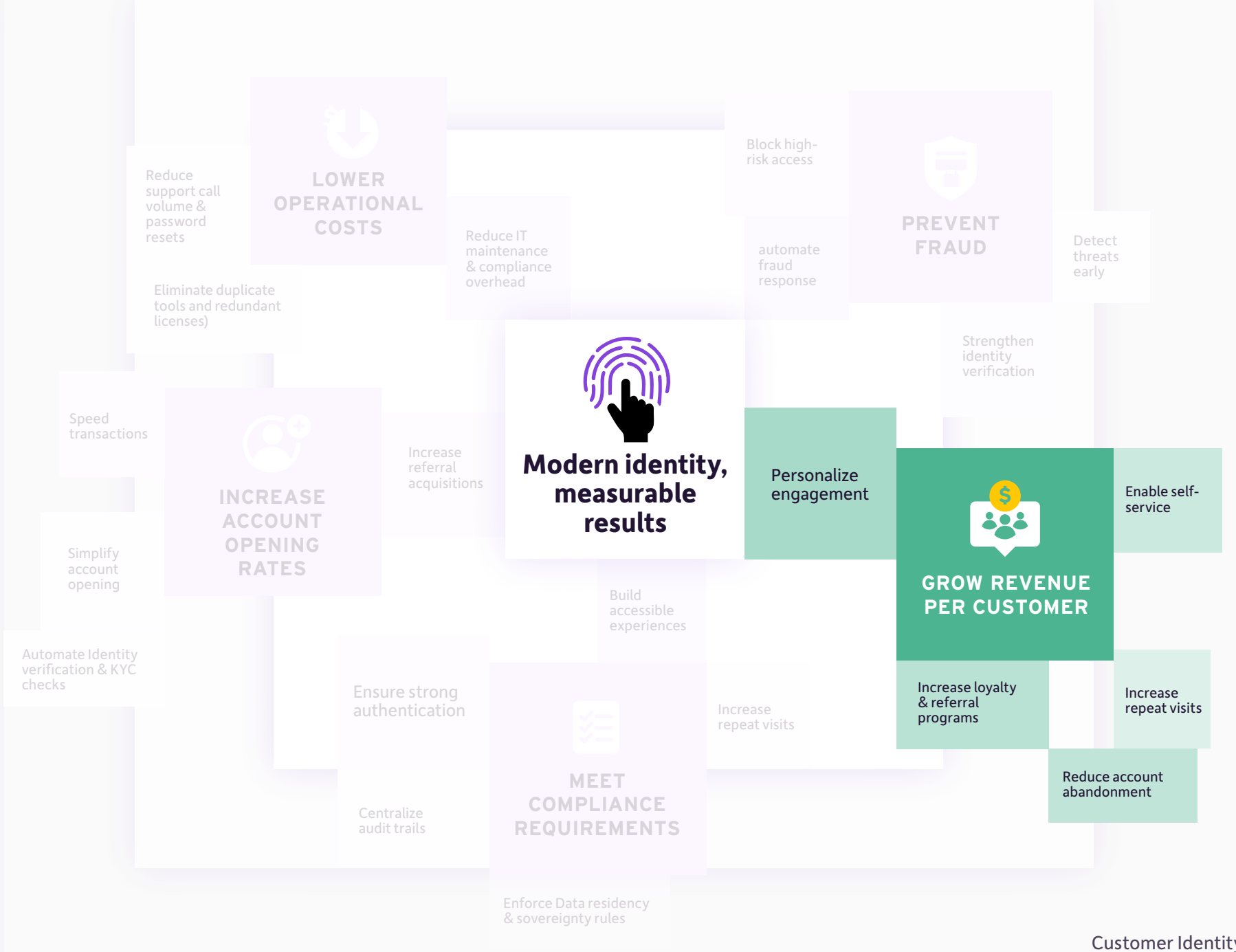
See the table below for metrics and how to measure them.

	Metric	Why it matters	How CIAM supports	How to measure
1	**Sign-up conversion rate**	A higher conversion rate means more prospects become customers	Simplified sign-up flows and secure login options reduce friction during onboarding	% of customers who start sign-up and complete account opening; A/B test layout and flows for sign-ups; Mean time spent on registration screens
2	**Onboarding abandonment rate**	Highlights where customers drop off during sign-up	Tracks drop-off at each step of onboarding, including verification	% drop-off at each step; A/B test to optimize step-by-step performance
3	**Time to first transaction**	A faster first action improves activation and increases long-term retention	Frictionless authentication, strong onboarding CTAs and product prompts post-login	Average time between account opening and first transaction or product use
4	**KYC and identity verification completion rate**	Verification delays cause friction and increase abandonment	Automated identity proofing and verification in flows to speed completion	% of customers completing KYC without escalation; % identity verifications pass/fail rates
5	**Referral conversion rate**	Referrals are a low-cost, high-trust acquisition channels	Secure, identity-aware referral links that track sign-ups from referrers	Referral invite-to-sign-up conversion rate
6	**Returning customer re-authentication success**	Customers return more often when sign-in is fast and frictionless	Risk-based access, biometrics, passkey support	% of returning customers who sign in successfully; % account lockouts or resets
7	**Segmented offer conversion**	Personalized offers increase sign-up rates among target audiences	Use identity data to personalize campaigns by segment, intent, or channel	Conversion rate by customer segment or offer type
8	**Fraudulent account sign-up prevention**	Prevents fraud while keeping sign-up simple for real customers	Real-time fraud signal detection, document verification, and device analysis	% flagged fraud accounts vs total sign-ups

4 Grow revenue per customer

The sign-in experience isn't just a security checkpoint, it's a revenue moment. Once a customer logs in, you've got a powerful opportunity to deepen the relationship, deliver personalized value, and increase share of wallet.

CIAM plays a critical role in turning passive customers into active ones, driving upsell, loyalty, and long-term engagement all while lowering acquisition costs.


LOWER OPERATIONAL COSTS
Reduce support call volume & password resets
Eliminate duplicate tools and redundant licenses)
Reduce IT maintenance & compliance overhead
PREVENT FRAUD
Block high-risk access
automate fraud response
Detect threats early
Strengthen identity verification
Modern identity, measurable results
INCREASE ACCOUNT OPENING RATES
Speed transactions
Simplify account opening
Automate Identity verification & KYC checks
Increase referral acquisitions
Build accessible experiences
Ensure strong authentication
MEET COMPLIANCE REQUIREMENTS
Centralize audit trails
Enforce Data residency & sovereignty rules
Personalize engagement
GROW REVENUE PER CUSTOMER
Enable self-service
Increase loyalty & referral programs
Increase repeat visits
Reduce account abandonment

Strategies to increase customer value

1

Personalize engagement using identity signals

Knowing who your customer is and what they need is the foundation of every high-value interaction. Unified identities let you tailor your customers account management experience, product recommendations, and content across web, mobile, and in-branch experiences.

Metric to track:

Cross-sell/upsell conversion rate post-login

2

Drive recurring usage through seamless access

Friction at login drives churn. Passwordless authentication, remembered devices, and biometrics help customers come back more often and stick around longer.

Metric to track:

Login frequency and session duration

3

Enable self-service product enrollment

Give customers the ability to discover and activate products without needing to call an agent. Streamlined enrollment drives higher adoption of cross-sell and upsell offers.

Metric to track:

% of users enrolling in products without assistance

4

Recover dormant or abandoned accounts

Forgotten credentials often lead to lost revenue. A strong CIAM platform supports secure, self-service account recovery that prevents abandonment and preserves lifetime value.

Metric to track:

Account recovery success rate and retention after recovery

5

Power loyalty and referral engagement

Engaged customers become advocates. CIAM helps power secure, compliant referral programs and enables personalized loyalty tracking all tied to a unified customer profile.

Metric to track:

Referral sign-up conversion and loyalty program opt-in rate

The bottom line:

A well-orchestrated identity experience doesn't just protect customer accounts, it grows them. The right CIAM strategies help financial institutions maximize the value of every customer who signs in, increasing revenue while building lasting trust.

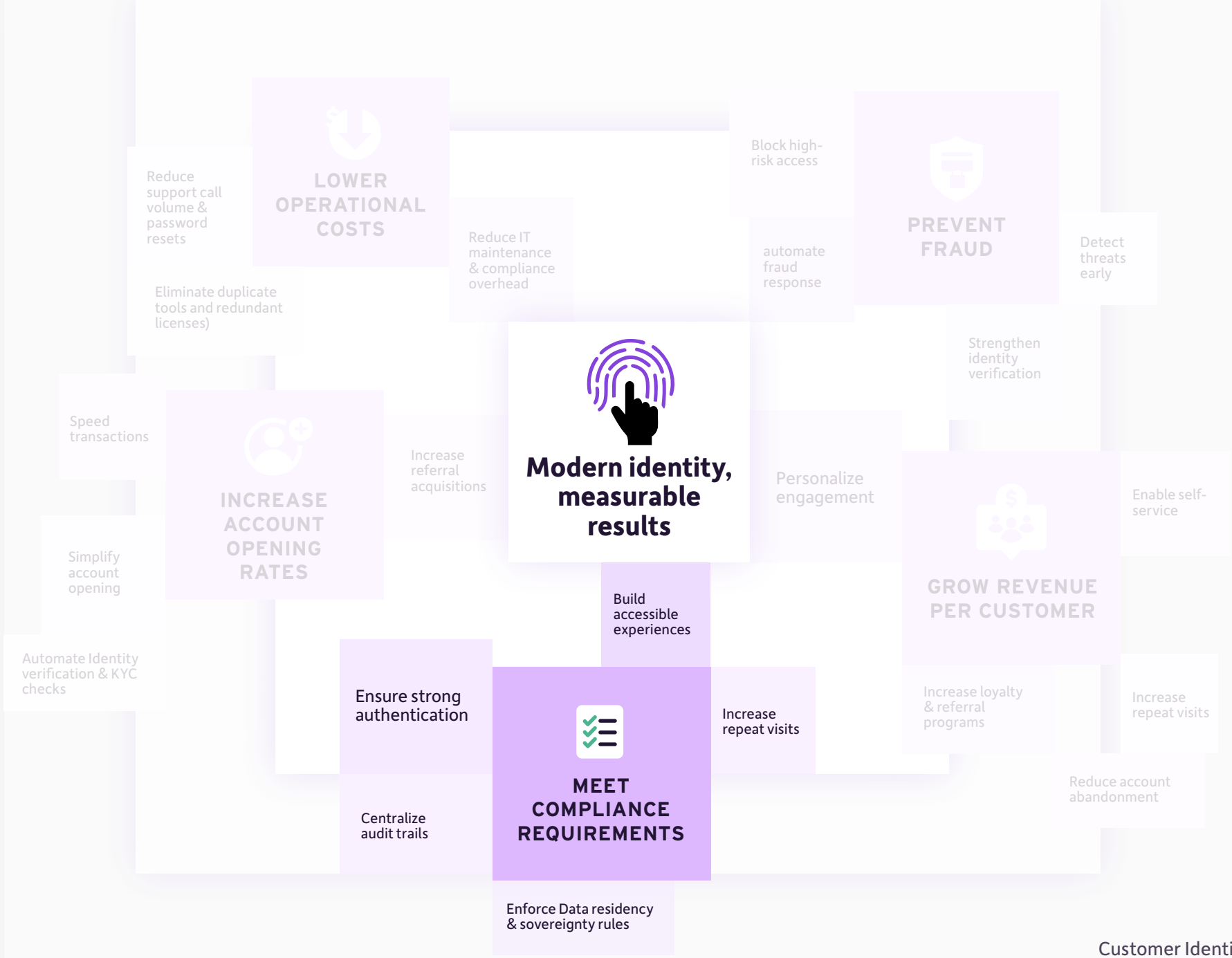
See the table below for metrics and how to measure them.

	Metric	Why it matters	How CIAM supports	How to measure
1	**Products per customer (PPC)**	Indicates relationship depth and drives long-term value	Unified identity and cross-product visibility enable access and tracking	Average # of accounts/products per customer
2	**Cross-sell/upsell conversion**	Expands wallet share with existing customers	Personalized post-login offers, progressive profiling, identity-driven targeting	% of customers accepting contextual offers post-login
3	**Digital engagement rate**	Frequent usage correlates with satisfaction, retention, and upsell readiness	Passwordless login, adaptive authentication, and progressive profiling for personalization	Login frequency, session duration, and repeat usage rates
4	**Customer lifetime value (CLV)**	Reflects overall customer profitability across the relationship lifecycle	Smooth onboarding, secure sign-in, and ongoing engagement across channels	Login engagement across touchpoints, purchase history
5	**Retention / attrition rate**	Lower churn means more sustainable revenue and better ROI	Consistent access and early churn signals like inactive or dormant accounts	Inactive customer logins and churn rate over a 12-month period
6	**Self-service product enrollment**	Reduces acquisition costs and accelerates product adoption	Easy access, Self-service capabilities, and unified identity across products/services	% of digital users enrolling in products without agent help
7	**Referral conversion rate**	Satisfied customers become advocates	Secure referral tracking, smooth onboarding, and login-based incentives	Referral sign-ups ÷ total referrals sent
8	**High-margin product adoption**	Premium products yield higher margins without new acquisition costs	Identity-based targeting for premium products	% of customers adopting higher-margin products
9	**Loyalty rewards program opt-in**	Entices customers to repeatedly engage and use your services	Consent and account management, fraud protection for reward abuse	% of customers enrolled in rewards % increase in revenue per rewards participant

5 Meet compliance requirements

Compliance pressure keeps rising but that doesn't mean your experience has to suffer. From GDPR to NYDFS, PSD2, and WCAG, modern CIAM helps you embed requirements directly into your sign-in flow without adding user friction.

With built-in logging, access control, consent management, and regional data handling, you can meet mandates efficiently and prove it at audit time.


LOWER OPERATIONAL COSTS
Reduce support call volume & password resets
Eliminate duplicate tools and redundant licenses)
Reduce IT maintenance & compliance overhead
PREVENT FRAUD
Block high-risk access
automate fraud response
Detect threats early
Strengthen identity verification
Modern identity, measurable results
INCREASE ACCOUNT OPENING RATES
Speed transactions
Simplify account opening
Automate Identity verification & KYC checks
Increase referral acquisitions
Personalize engagement
GROW REVENUE PER CUSTOMER
Enable self-service
Increase loyalty & referral programs
Increase repeat visits
Reduce account abandonment
Build accessible experiences
Ensure strong authentication
Increase repeat visits
MEET COMPLIANCE REQUIREMENTS
Centralize audit trails
Enforce Data residency & sovereignty rules

Strategies to reduce compliance risk

1

Centralize consent and audit trails

Many banks still manage consent and audit data in fragmented systems, a recipe for compliance gaps. A modern CIAM platform captures and versions consent at login or registration, logs account activity, and creates tamper-proof records.

Metric to track:

% of users with valid consent logs; time to generate audit report

2

Enforce secure access without creating friction

Regulations like NYDFS, PSD2, and GLBA require strong customer authentication. CIAM helps you meet these mandates with adaptive MFA, risk-based step-up, and passkeys to improve both security and usability.

Metric to track:

MFA adoption rate and failed login attempts by authentication method

3

Build accessibility into every login flow

Standards like ADA, Section 508, and WCAG require that all users, including those with disabilities, can access digital services independently. CIAM platforms ensure login screens and recovery flows support screen readers, keyboard navigation, and high-contrast modes.

Metric to track:

Accessibility test success rate and audit readiness

4

Respect data residency and sovereignty rules

GDPR, PIPEDA, and APAC data laws require you to store and process data regionally. CIAM gives you control over where identities live and how they're handled with location-specific backup, audit, and processing options.

Metric to track:

% of customer data stored within required regions

5

Enable rights management and portability

GDPR and CCPA grant users the right to access or delete their data. Modern CIAM supports automated deletion and export flows, complete with logs to prove fulfillment within SLAs.

Metric to track:

Fulfillment time for deletion/export requests and error rates

The bottom line:

You don't have to sacrifice user experience to meet regulatory requirements. With the right CIAM capabilities, you can build compliant, audit-ready customer journeys that also feel seamless, accessible, and secure.

See the table below for metrics and how to measure them.

	Metric	Why it matters	How CIAM supports	How to measure
1	**Consent logging & management**	Required by GDPR, CCPA, NYDFS, and others to track how customer data is collected and used	Centralized, versioned consent tracking with user access and export options	% of users with valid, up-to-date consent logs; audit trail completeness
2	**Access control & least privilege**	Regulatory frameworks require tight control over access to customer data	Role-based access control and policies to restrict admin/system access	Number of overprivileged accounts; access review frequency
3	**MFA adoption rate**	Mandated by PSD2, NYDFS, and other laws to protect against unauthorized access	Adaptive MFA, passkey support, and step-up authentication based on real-time risk	MFA adoption rate; step-up prompt frequency; failed login rates by method
4	**Data residency & sovereignty**	Laws require personal data to remain in-region (e.g., EU, APAC, Canada)	Region-specific CIAM instances with configurable data storage and backup locations	% of customer data stored in allowed regions; geo-location audit verification
5	**Audit logging & reporting**	Compliance audits require detailed, tamper-proof activity records	Centralized logs of auth events, consent changes, admin access, and fraud signals	Time to generate audit report; % of audit trails with complete data
6	**Breach detection & notification**	Regulators impose strict timelines to notify breaches	Real-time detection of anomalous login behavior and credential-based threats	Mean time to detect and respond to authentication related threats
7	**Identity verification at onboarding**	Prevents fraud and ensures regulatory KYC compliance	ID verification, phone/email/address validation, and IP/device reputation checks at sign-up	% of verified users; account rejection rate due to risky attributes
8	**User data portability & deletion**	Required under GDPR and CCPA "right to be forgotten" laws	Self-service account export/deletion, backed by workflow and compliance audit logs	% of deletion/export requests fulfilled within SLA; error rate in data exports
9	**Accessibility**	Required under ADA, Section 508, EAA, WCAG and similar regulations	Compliant login and registration flows with keyboard navigation and screen-reader support	% of audits passed; screen reader test success

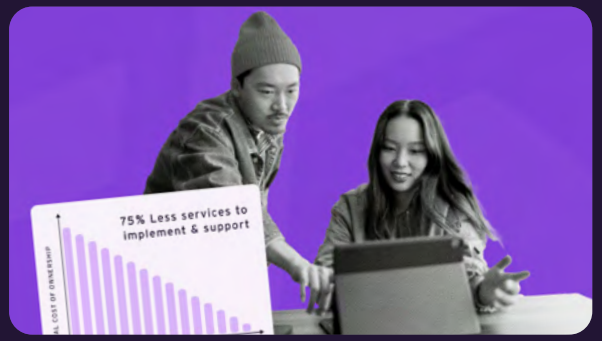
Want to learn more?

Take the next step toward optimizing your identity journeys.

Explore our Customer Insights page

See how we help teams use identity data to identify friction points, reduce drop-offs, and improve sign-in and sign-up performance.

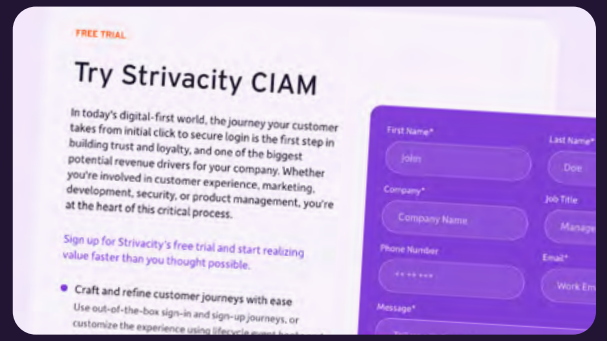
https://www.strivacity.com/capabilities/customer-insights ↗



Request a free Customer Journey Assessment

Our experts will review your current sign-up and sign-in experience to identify quick wins and longer-term opportunities.

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



Thinking of replacing your existing CIAM provider?

Explore how we help organizations move away from legacy platforms.

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

Customer Identity Metrics Mind Map for Financial Services

The ultimate guide to measuring customer identity journeys that drive growth, reduce risk, and improve compliance

ABOUT US

Strivacity helps brands add secure sign-up and sign-in capabilities to their customer-facing applications without tying up a crew of developers or consultants. We offer a unified customer identity and access management (CIAM) solution that uses clicks (not custom coding) so organizations can get going fast and don't have to choose between creating great customer experiences, securing their customers' data and staying compliant with fast-changing privacy regulations like GDPR and CCPA. To learn more about Strivacity, visit www.strivacity.com.

205 Van Buren Street
Suite 120
Herndon, VA 20170

+1 844 782 5486 strivacity.com