Guide

Retail Series | 2

How to balance compliance and personalisation in a privacy-conscious world

okta

Introduction

In 2024, roughly 22% of global retail sales are expected to occur online — a significant jump over 2019's pre-pandemic figure of only 15%. And online's share is expected to increase, with projections suggesting e-commerce will account for 24% of an $8.1 trillion dollar global market by 2026.

But even as consumer spending surges, retailers face strong headwinds:

- Every retailer – no matter how big or how small – now competes in a truly global marketplace
- Rampant inflation and rising interest rates are putting the squeeze on customers' disposable income, further intensifying competition among retailers
- With an increase in online shopping comes an increase in returns, forcing many retailers to explore fees to cover soaring shipping and processing costs

To attract and retain customers, retailers worldwide are exploring store makeovers, pop-up stores, celebrity partnerships, loyalty programs, and other promotions. Behind the scenes, many are also engaged in merger and acquisition activity and are investing significantly in transformative technologies.

As eCommerce and retail businesses evolve, managing digital Identities is an increasingly critical function. When the right Customer Identity and Access Management (CIAM) platform is implemented, retailers can optimise operations, organisational processes, and marketing programs to delight customers with personalised experiences at every touchpoint – from product discovery to purchase and beyond.

While the literal definition of CIAM has remained consistent over the years, its true meaning and impact have evolved as digital transformation has changed how customers and retailers build relationships and interact.

> "With digital transformation and pressure to build orchestrated Identity into the customer journey, CIAM solutions are an essential building block of customer management."
>
> The Forrester Tech Tide™: Identity And Access Management (IAM), Q1 2023

A modern CIAM platform allows retailers to leverage data and create meaningful relationships with customers, tackle the problem of fragmented data, satisfy customer demands for data privacy, and even help reduce instances of fraud and other security issues.

In this guide – which is one piece of a five-part collection – we'll focus on CIAM's role in balancing compliance and personalisation in a privacy-conscious world.

Acquiring, managing and leveraging customer data is getting harder

The fifth edition of Salesforce's State of the Connected Customer report revealed that 73% of consumers expect companies to understand their unique needs and expectations (up from 66% in 2020).

Most marketers are happy to oblige, but delivering personalised experiences and crafting high-performing campaigns requires information – and many traditional data sources are disappearing:

- Cookies are disappearing (even if Google has pushed out their Privacy Sandbox initiative a few times)
- Legislation (e.g., the EU's GDPR, California's CCPA, Brazil's LGPD, Japan's APPI, Australia's Privacy Act, Singapore's PDPA, etc.) is giving consumers additional rights with regards to their personal data
- Technology companies have introduced anti-tracking measures – most notably Apple's App Tracking Transparency (ATT), which reportedly cost Facebook $10 billion in lost revenue
- Companies are also pushing back against browser fingerprinting – a way of uniquely identifying an individual without using a tracking cookie – with Apple and Mozilla including anti-fingerprinting measures by default

> "Every marketer shudders at the thought of a cookieless world. Cookies allowed us to be passive observers, collecting buckets of data that we could use at every stage of the customer journey."
>
> **Kerry Ok**, Chief Marketing Officer, Okta

In the privacy-conscious cookieless age, campaigns and personalised experiences will be powered not by third-party data but instead by customer consent. In this new paradigm, terminology needs to evolve so that marketers can distinguish between:

- Zero-party data that customers willingly share with you, such as fields on a sign-up form, their shipping details, or an email survey they completed. This often includes personal data that can be attributed to a single person and is usually protected by data privacy regulations.
- First-party data that customers generate as they consent to interact with your site, including search history, analytics information, session metadata, and more. Unlike zero-party data, first-party data is often anonymous.

CIAM is the key to acquiring, managing, and leveraging this data – and to enabling Identity resolution – while meeting ever-evolving customer expectations and regulations.

Enriching profiles while meeting customer expectations for privacy

Today's customers prioritise privacy, as demonstrated by Okta's Customer Identity Trends Report. Based on a survey of 21,512 consumers from 14 countries, the report revealed that:

- The large majority of customers – about 71% – are aware that their online activities leave a data trail, and most of that majority report taking steps to mitigate it
- More than three-quarters of Retail & Hospitality customers – 77% globally – consider having control over their data (e.g., changing privacy settings, limiting the information you have to share) to be "somewhat" or "very" important (Figure X)

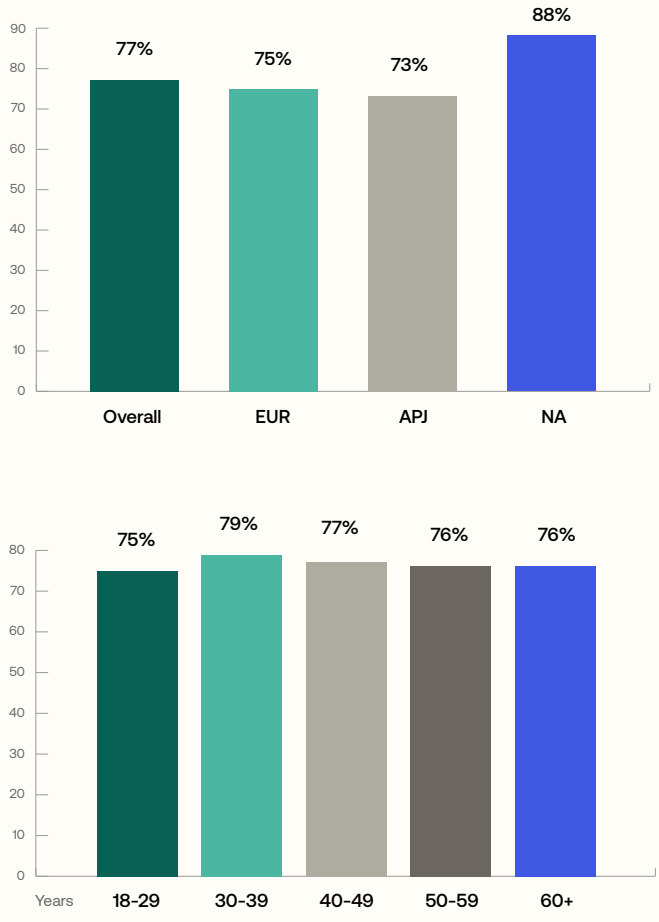

Figure X: When interacting with a brand online, how important is it to you to have control over your data (e.g. change the privacy settings, limit the information you have to share)? (Retail & Hospitality industry, sum of Very Important and Somewhat Important)

Given the strong competition for customer attention – and the strong trend towards increased regulation around privacy – brands that want to build long-term customer loyalty should be transparent about what data is needed and how it's used to power a private, secure, and convenient experience, and should provide customers with tools to manage their preferences.

But in a privacy-conscious world, how do you persuade customers to part with it in the first place?

The key is trust: customers will only share data and opt into marketing programs if they feel confident that their data is safe, is used in the way they've agreed to, and will benefit them by providing more personalised and convenient interactions.

> "Prioritising transparency and privacy means being transparent about data collection and use, offering opt-out options, and adhering to privacy regulations."
>
> **Matt Duench**, Senior Director, Product Marketing, Okta

CIAM is the foundation for all of these things.

For example, data privacy regulations often require you to obtain customers' explicit consent to their data being collected and used. CIAM helps you manage this more easily by simplifying how consents are requested, stored, and updated across all your channels. This level of clarity and control also helps you easily respond to consumers' enquiries – or proactively communicate policies in plain language – regarding what data you store for them.

Similarly, data is vital for tailoring your offers, remembering your customers, and reducing the need for them to re-enter information – but how you gather data can make or break customer perceptions and experiences.

When asked what issues have the potential to frustrate them the most when registering or logging in to a Retail & Hospitality service, 49% of respondents to the Customer Identity Trends Report survey selected "Filling up long login or sign-up forms" – making it far-and-away their biggest annoyance.

CIAM enables you to utilise progressive profiling, in which you gradually build up a picture of your customer in a way that establishes trust. By collecting data incrementally and with your customer's full consent, you can confidently collect zero-party data to segment, tailor, and personalise marketing efforts – all while contributing to a positive customer relationship.

And what about storing the data in a manner that complies with regulations?

Again, CIAM offers the answer with secure-by-design solutions that empower retailers to meet data residency requirements.

Enabling a holistic view of every customer

Thanks to the proliferation of digital channels, marketers now potentially have a vast amount of data at their fingertips. Every online interaction tells you more about your customers, whether that's their demographics, behaviour patterns, preferred communication channels, favoured products, or buying habits.

The problem is that data may be inconsistently gathered and scattered across disparate systems, giving you an incomplete picture of the truth.

The same customer may have multiple Identities on multiple platforms and brands, all owned by your organisation. For example, they may have a separate account for your online store and another for your loyalty program. Or their information may not have been gathered in compliance with data protection regulations, making it untrustworthy and unusable.

Plus – as noted earlier – first-party data is often collected anonymously. In many retailers, it stays in a web analytics system rather than being incorporated into a database with known customers.

Without tying your data to known, engaged, and converted customers, potential treasure troves of information are wasted. You know little about your buyers, what they like, or how they've interacted with you before.

That's where CIAM comes in: when connected to your Customer Data Platform (CDP), Customer Relationship Management (CRM) solution, or other marketing and business systems, CIAM enables a single, holistic, 360-degree view of every customer, allowing you to:

- Perform Identity resolution to recognise individual users – perhaps with multiple email addresses and phone numbers – across devices and channels
- Understand their journeys and behaviours across all your digital channels
- Enrich their profiles with trusted, compliantly gathered data and use it to deliver tailored offers
- Improve the performance of your campaigns by revealing which customer segments and profiles are likely to respond positively to specific marketing messages or promotions

How to get started

Because CIAM sits at the heart of customer-facing systems – serving as an input into market analysis and influencing acquisition, conversion, and retention efforts – it aligns with marketing and customer experience departments.

At the same time, CIAM directly impacts security and privacy, putting it squarely in the sights of CISOs, CIOs, and compliance officers.

And – fundamentally – CIAM is a set of technology solutions, causing it to fall under IT organisations or even CTOs (when properly regarded as an enabler of digital transformation).

To find the right balance between the quality of customer experience and system security in the context of desired use cases, customer types, data types, and retail-specific factors, leaders across these functions should work together to implement CIAM.

Here are some suggestions for getting started as you look to balance compliance and personalisation in a privacy-conscious world:

- **Reassure customers about trust and privacy**
  Deploy features that boost authentication security – like passkeys and MFA – and give your customers control over what data they share and how it will be used.

- **Determine how you will manage customer consent**
  Acquiring customer consent to collect and use data is already required in many jurisdictions and will become so in others – modern CIAM systems integrate with consent management tools to make this task easier.

- **Implement a progressive profiling strategy**
  Allow a customer to create an account with only basic information, then gradually ask for more details as the relationship grows.

- **Integrate your CIAM system with your CDP**
  Customer data platforms can be invaluable within the larger marketing technology stack, but they need reliable data – integrating your CIAM system with your CDP helps to ensure data is associated with real customers and makes it easy to combine the zero-party data captured during the sign-up process with the first-party analytics data generated elsewhere.

- **Protect customer Identity data**
  In addition to basic hygiene like encrypting data and limiting access to it, look for a CIAM solution that includes features to defend against Identity-related attacks like fraudulent signups and account takeovers (e.g., via credential stuffing).

Find out more about CIAM's role in retail

This mini guide is one of a five-part collection, each of which focuses on a different application of CIAM within the retail space.

Discover the rest of the series on the landing page link below.

Learn more in APJ

Learn more in EMEA

Estimate the revenue gain of using a Customer Identity solution

Visit **this page** to calculate how Okta can help your retail business improve customer conversion rates and increase profitability.

Discover more about Identity management with Okta

Building and maintaining an effective Identity solution – one that empowers and enables your business, rather than holds it back – is a huge undertaking.

Okta is the World's Identity Company and is helping retailers all over the world deliver exceptional digital experiences and understand their customers better, all whilst keeping their data safe.
Visit **okta.com** to learn more.

About Okta

Learn more at: www.okta.com Okta is the leading independent provider of Identity for developers and the enterprise. The Okta Identity Cloud securely connects enterprises to their customers, partners, and employees. With deep integrations to over 7,000 applications, the Okta Identity Cloud enables simple and secure access for any user from any device.

Thousands of customers, including 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn, and News Corp, trust Okta to help them work faster, boost revenue and stay secure. Okta helps customers fulfil their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

okta