CUSTOMER IDENTITY AND ACCESS MANAGEMENT (CIAM)

ULTIMATE GUIDE

Ultimate Guide to Customer Identity and Access Management

TABLE OF CONTENTS

CHAPTER 01

IT'S (STILL) ALL ABOUT CUSTOMER EXPERIENCE

It was 2015 when Gartner said that customer experience (CX) had become the new competitive battlefield, and that statement stands true today. More than ever, CX holds the potential to help you acquire new customers and make raving fans out of the ones you already have.

But the reality today is that most organizations are still struggling to deliver the connected customer journey required for exceptional CX. While that customer journey will look slightly different for each organization, the need to make transitions between each step of the journey as seamless as possible is universal. And you don't get many chances to get it right.

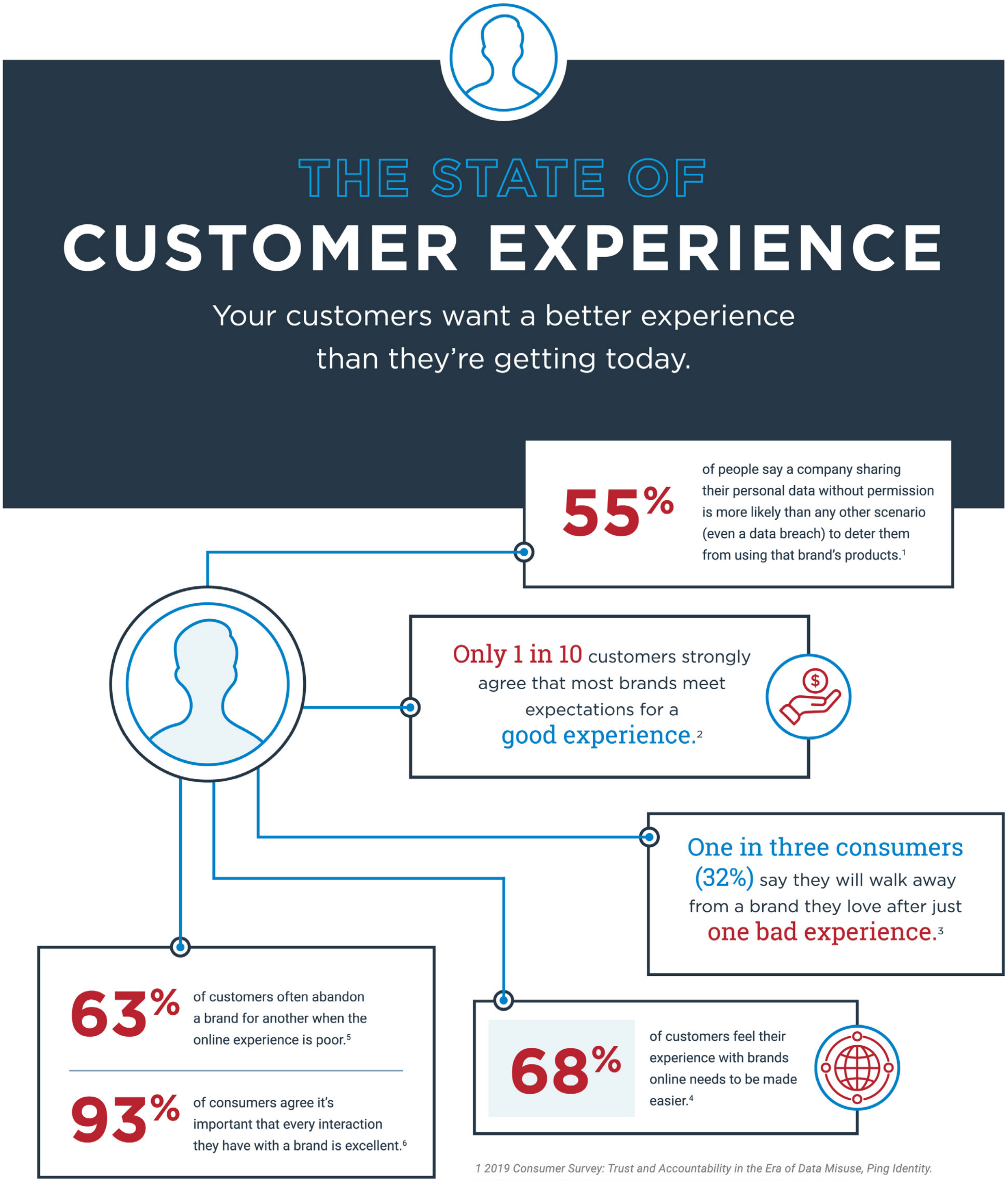
Customer identity can help you ensure that every stage of your customer's journey is seamless and delivers the experience they expect. But it's a double-edged sword. Without a well-conceived approach, identity can also be the source of friction. If your customers find things like registration, sign-on and updating preferences to be complex or cumbersome, they may abandon your brand.

> Companies will win or lose based on experience, and CX is still the vital point of differentiation and growth.
>
> SOURCE: FORRESTER

The sweet spot lies in harnessing the power of customer identity wisely and to your greatest advantage. When done correctly, identity can set the foundation for the exceptional CX required to win the battles for customer acquisition, retention, revenue, loyalty and trust

So how do you get identity right? Read on to gain a deeper understanding of:

- Your customer's expectations of you
- The role identity plays in the customer journey
- How to use identity wisely to deliver the CX your customers want



THE STATE OF CUSTOMER EXPERIENCE

Your customers want a better experience than they're getting today.

55% of people say a company sharing their personal data without permission is more likely than any other scenario (even a data breach) to deter them from using that brand's products.[1]

Only 1 in 10 customers strongly agree that most brands meet expectations for a good experience.[2]

One in three consumers (32%) say they will walk away from a brand they love after just one bad experience.[3]

63% of customers often abandon a brand for another when the online experience is poor.[5]

93% of consumers agree it's important that every interaction they have with a brand is excellent.[6]

68% of customers feel their experience with brands online needs to be made easier.[4]

[1] *2019 Consumer Survey: Trust and Accountability in the Era of Data Misuse, Ping Identity.*
[2] *Deliver the CX They Expect: Customer Experience Trends Report, Acquia.*
[3] *Experience is everything: Here's how to get it right, PwC.*
[4] *Deliver the CX They Expect: Customer Experience Trends Report, Acquia.*
[5] *2019 Consumer Pulse Survey, Accenture.*
[6] *Ibid.*

CHAPTER 02

CUSTOMER EXPERIENCE: WHAT YOUR CUSTOMERS REALLY WANT

Managing the customer experience across the entire journey can feel like a tall order. But what your customers really want is simple:

- Delight me
- Protect and respect me

Delight Me

Things like registration and sign-on are a necessary part of a digital customer experience. But they aren't the parts your customers enjoy, and that's all the more reason to make them as seamless and convenient as possible.

If you make these initial interactions too cumbersome, you run the very real risk of driving customers away. But when you provide simple and secure access, it's like rolling out a virtual red carpet that invites them in. This is the type of CX that delights your customers and paves the way for increased engagement.

> Customers...will respond to brands that show interest in them and their feelings and then follow that up with a consistent, technology-driven experience.
>
> SOURCE: "FIVE TRENDS SHAPING THE FUTURE OF CUSTOMER EXPERIENCES IN 2020," FORBES

Multi-channel: Don't Make Me Tell You Twice

The channels through which you deliver customer experience have become increasingly complex as digital tools have evolved. But at the end of the day, your customers want good old-fashioned customer service. They want that feeling you get when you walk into your local coffee shop and the barista greets you by name and has your drink almost made by the time you get to the counter.

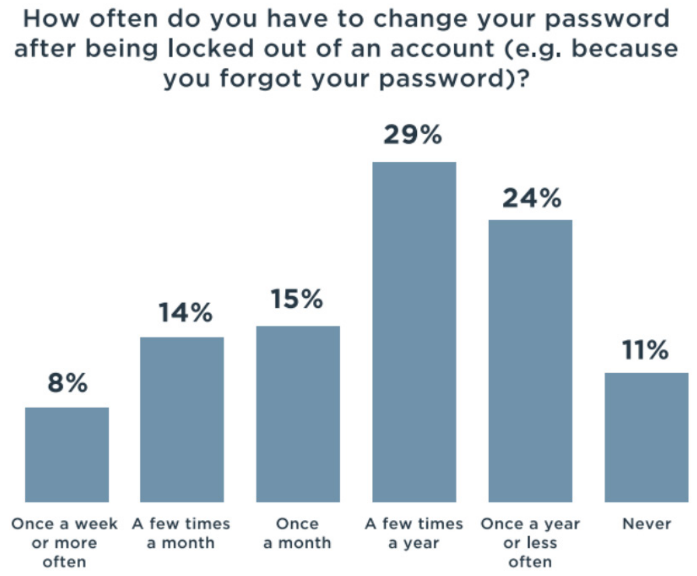
Said another way, your customers expect to be able to communicate something once and have you remember it. This means if a customer changes their name on their checking account, they expect you to make the change on their associated savings and investment accounts as well. Similarly, if a customer updates their preferences to opt-out of emails on your mobile application, they expect that your web application doesn't email them either. Sure, these functions may be managed by separate teams within your organization or external third parties, but your customers don't know this, nor do they care.

Read the white paper to learn more about delivering seamless multi-channel experiences.

Frictionless: Don't Make Things Harder than Needed

When you're unable to deliver the consistency customers want, you introduce friction. Friction can be anything that impedes a customer along their journey, from small annoyances to bigger disconnects. A classic example is complicated password policies.

In an attempt to maintain security, some organizations require users to create very long passwords that contain specific combinations of capital letters, numbers, and symbols. This is an area where a balance between convenience and security is critical. If policies are unnecessarily complex it can be difficult to come up with a password initially, let alone enter it twice without making a mistake.



A 2019 survey of more than 4,000 consumers in the U.S., UK, Australia, France and Germany found that 37% of customers must change a password at least monthly because of account lockout.

Remembering these intricate passwords is just as difficult, leaving many customers in the position of having to reset their forgotten passwords every time they log in. Expecting that your customers will continue this dance is unrealistic. More likely, they'll abandon your brand in favor of organizations that offer a smoother experience.

Are your authentication methods driving customers away? Read the blog to discover 5 common authentication mistakes—and how to fix them.

Fast: Don't Waste My Time

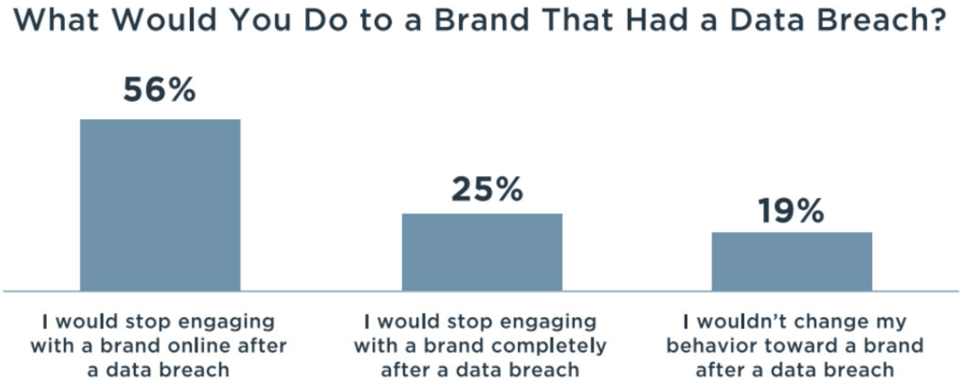
Poor experiences like complicated password requirements aren't just frustrating, they take too much time. Like Mr. Vain in the '90s song by Culture Beats, your customers know what they want and they want it now. They don't want to go through additional steps or processes. In cases where security is crucial, such as banking, it's okay to require more from customers. The key is not to require more than is necessary, so you can make access as hassle-free as possible.

Now, you may know what it really takes to deliver that type of experience. But as a gentle reminder, no one comes to your site to see how awesome your registration or sign-on experiences are. In fact, the way you know those experiences are amazing is when they're so seamless they go completely unnoticed.

Protect & Respect Me

Data security has become a major concern for consumers in recent years. Whether justified or not, your customers are placing the sole responsibility for data protection on you and expect more accountability than ever.

As more and more digital information is gathered about customers, their concept of security has also evolved. Protecting them from breaches and fraud alone isn't enough. Your customers also expect you to respect their privacy and be good stewards of the data they share with you.



The 2019 Consumer Survey "Trust and Accountability in the Era of Data Misuse" revealed that 81% of customers would limit or completely stop their interactions with a brand following a breach.

> ""
>
> Ensuring that [your] brand won't lose or abuse their data, and recognizing consumers in a way that puts them at ease are all part of a better experience.
>
> SOURCE: ACCENTURE 2019 CONSUMER PULSE SURVEY

Breaches: Don't Expose My Personal Data

Data breaches are among the most costly events a customer-facing enterprise can experience. A single breach can result in customer abandonment, fines, and brand damage that is nearly impossible to quantify. Our 2019 survey of more than 4,000 customers across the U.S., UK, Australia, France and Germany found that 56% would stop engaging with a brand online following a breach and an additional 25% would stop all interaction whatsoever.

If you're storing user data, you have the responsibility for protecting that data. That includes ensuring that potential bad actors both from outside as well as within your organization can't access the keys to the kingdom. Your customers are trusting you to take the security measures needed, no matter what it requires.

Fraud: Don’t Put Me at Risk

Our 2019 survey also revealed that 63% of customers believe a company is always responsible for protecting their data. This is regardless of whether they fell victim to a phishing email or did something unsafe like using unencrypted Wi-Fi connections or the same password across accounts. Said another way, most customers will blame you if they fall victim to fraud even if there was little or nothing you could have done to prevent it.

While incidents of fraud don’t make headline news as often as big breaches do, these more narrowly targeted attacks impact the individual much more acutely. And the onus is on you to make sure whoever is requesting access really is who they say they are. Given what’s at risk, usernames and passwords aren’t enough, and any defense you can mount is well worth it.

> 49% of people are more concerned about protecting their personal information today than they were one year ago.
>
> SOURCE: 2019 CONSUMER SURVEY: TRUST AND ACCOUNTABILITY IN THE ERA OF DATA MISUSE

> 55% of people say a company sharing their personal data without permission will deter them from using that brand’s products.
>
> SOURCE: 2019 CONSUMER SURVEY: TRUST AND ACCOUNTABILITY IN THE ERA OF DATA MISUSE

Privacy Violations: Don’t Disrespect Me

Across industries, customers are skeptical about companies’ ability to protect their privacy. Even as customers increasingly see the value in choosing security over convenience, their top priority is that their privacy be maintained—and respected.

While regulations like GDPR and CCPA further support this expectation, they also provide an opportunity to demonstrate this respect. It’s all too easy to see compliance as just another hurdle to overcome. But when you give customers transparent insight into and control over the personal data you’ve gathered about them, you’re also giving them the respect they expect and in doing so earning their trust.

Read the blog to learn more about building customer trust with privacy and consent.

Balancing Convenience, Security and Privacy

Customers value security, convenience and privacy. There is no perfect balance. The ideal mix will vary from organization to organization. Finding the mix that's right for you is a tall order, but customer identity helps you develop a plan that considers which conveniences are imperative, what risks you're willing to accept and ensures compliance with privacy regulations.

5 Ways to Defend Customer Data in the Digital Age

Given the many threats today's enterprises face, building a strong defense is a must. But some days it feels like a battle you can't win. Protecting customer data against breaches and fraud adds another layer of complexity to an already huge responsibility—and it requires different methods. Here are five things you can do to prevent attacks and limit the damage if one occurs.

1

Implement customer MFA

Customer multi-factor authentication provides a greater level of assurance that the user accessing an app is actually your customer, not someone who successfully phished them. Should access be attempted with a stolen username and password, the customer will be prompted on their trusted device to complete authentication. This alerts the customer their credentials have been compromised and in doing so can thwart the attack.

2

Control access to your APIs

While APIs are driving digital transformation, they're also attractive targets for hackers and rogue insiders. You can protect against common gaps in API security by securing access to your APIs and restricting access to only the data that's needed.

3

Encrypt data

To protect customer information, you need a secure place to store their data. But you also need the ability to protect data while in use and in motion. Enforcing data encryption allows you to protect data at all times so if it does end up in the wrong hands, it's unusable.

4

Implement workforce MFA

The 2019 Verizon Data Breach Investigations Report found that 34% of data breaches were inside attacks, whether innocent or intentional. Modern workforce multi-factor authentication gives you the added assurance that users are who they say they are, wherever, whenever and however they need access to company resources like customer data and other sensitive resources

5

Monitor administrative activity

Breaches are often executed over time and can remain undetected for months or even years while customer data is slowly siphoned. By applying preventative controls like limiting the number of identities an administrator can download, tracking when logs are changed or creating alerts for other admin account escalations—you can effectively monitor suspicious activity and prevent attacks.

Protecting customer data may feel like an uphill battle, but these five tactics will help you mount a strong defense.

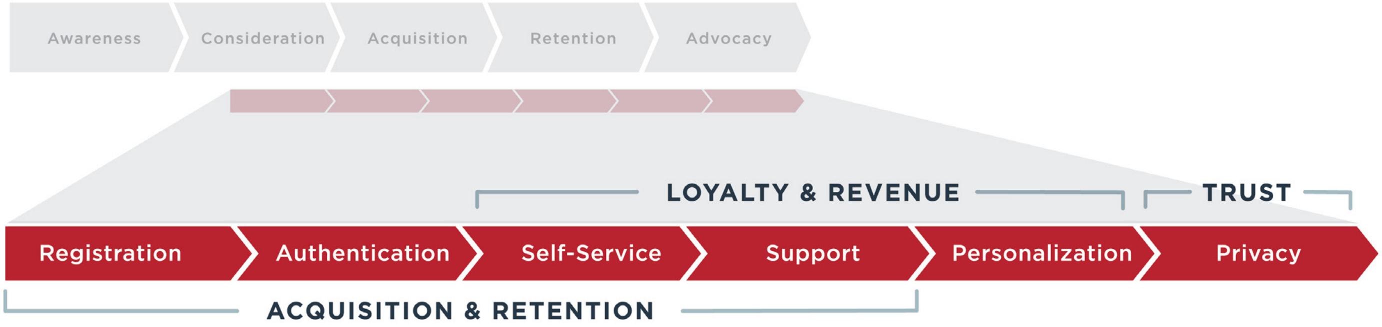
Watch the video to learn more about protecting customer data and enforcing consent.

CHAPTER 03

CUSTOMER IDENTITY: DELIVERING THE EXPERIENCE YOUR CUSTOMERS EXPECT

To deliver the CX your customers expect, you must deliver a seamless and secure experience beginning with your customer's first interaction with your digital properties and continuing throughout their journey.

The typical customer journey spans across several stages. This is often depicted as a linear progression starting at initial awareness and ideally culminating in advocacy as shown here.



Identity plays a critical role in the customer journey, supporting your ability to acquire and retain customers, build loyalty and revenue, and earn trust.

> Brands need to focus on consumers' experience at every interaction in the customer journey, from websites and mobile apps to physical stores.
>
> SOURCE: ACCENTURE 2019 CONSUMER PULSE SURVEY

The first stages are typically owned by the marketing function. As a customer progresses through these early stages, they could have dozens of interactions with your brand and digital properties, requiring significant investment of marketing dollars to deliver. Your organization has spent a lot of money to get prospects to this phase, so you don't want to fall down now.

Identity might play a minor part in the initial customer journey. For example, you could store anonymous user data before the customer registers. But identity plays a much larger role after registration occurs, marking the pivotal point where a visitor becomes a known user. Wherever identity enters into the equation for your customer's journey, it plays a critical role from that point forward by supporting your ability to acquire and retain customers, build loyalty and revenue, and earn trust.

Registration

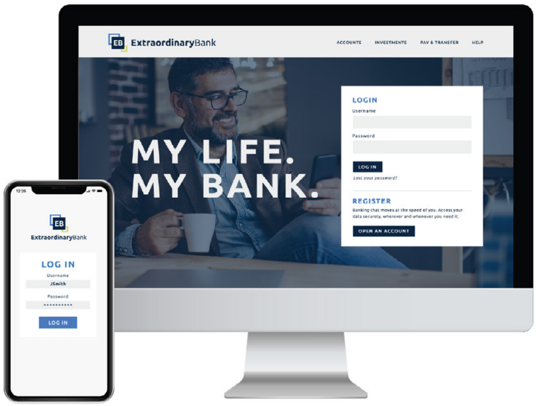
The experience your customer has at registration forms their all-important—and often very first—impression. Getting this wrong can cause new users to abandon your registration form, and cost you future revenue. To delight your customer, you must provide fast and frictionless registration by limiting the information gathered to only what's necessary, or offering alternate registration methods like social registration or the ability to register with third-party identity providers

Objective: Make registration fast and frictionless

How identity addresses it:

- Support for a number of registration options (social registration, standard fields or registration with other identity providers)
- Giving users single sign-on (SSO), creating a common registration experience and one set of credentials to access all apps
- Customizable registration pages to reflect your brand
- Convenient and secure password policies

Example: Instead of asking your customer to fill out a cumbersome registration form, provide the ability to register with their Facebook or Google account.



Banking that moves at the speed of you. Access your data securely, wherever and whenever you need it.

The ability to customize authentication experiences either through customizable templates or APIs is critical.

Authentication

Authentication is how you ensure your customers are who they claim to be during every subsequent interaction with your digital properties. But they don't want to go through a painful or inconvenient authentication process to prove their identity. Despite login needing to be very easy for users, it needs to be very difficult for hackers to get past. That's why multi-factor authentication (MFA) is becoming more and more necessary for customer applications, you can't expect customers to carry around a hard token or even download a third-party app, such as Google Authenticator. If you make authentication too cumbersome, your customers are more likely to abandon login and interact less with your brand, which ultimately equates to lost revenue.

> By 2022, 60% of large and global enterprises, and 90% of midsize enterprises will deploy passwordless verification.
>
> SOURCE: "EMBRACE A PASSWORDLESS APPROACH TO IMPROVE SECURITY," GARTNER

Objective: Make sign-on simple for any application

How identity addresses it:

- Single sign-on (access to all apps with one set of credentials
- Multi-factor authentication/adaptive authentication that balances convenience and security
- Multiple ways for customers to authenticate
- Passwordless login

Example: Instead of having to create separate login forms and credentials for different applications, your customer has one consistent sign-on experience for all of your company's brands or offerings.

Explore passwordless authentication options today with PingZero.

Passwordless Authentication: Maximizing Connectivity, Minimizing Friction

Your customers don't want authentication to be too cumbersome. And they don't want to navigate different sign-on experiences for each of your digital properties either. This is where passwordless authentication comes in.

For some, passwordless authentication may seem a little out there or unattainable, but it's born out of the same principles as multi-factor authentication. While MFA asserts that passwords alone aren't secure enough to prove identity and relies on additional authentication factors (like a trusted device), passwordless takes this a step further by eliminating passwords altogether and instead relying solely on more secure and more convenient factors.

Self-service

Your customers don't want to call or email to make basic changes to their account information. A core identity capability, self-service allows your customers to update and manage their personal information themselves, like changing a mailing address, email address or phone number. But that's not all. Your customers also need the ability to make changes once and have them applied to every application.

Objective: Make it easy to access and manage profile data once and have it reflected across channels

How identity addresses it:

- Synchronizing updated information and preferences across any and all user directories as soon as they're updated by the customer
- Allowing all apps to access a single source of truth about your customers

Example: When a customer updates their address on a banking mobile app, it's automatically updated on their check-ordering app so they don't need to make this change again when they place their next check order.

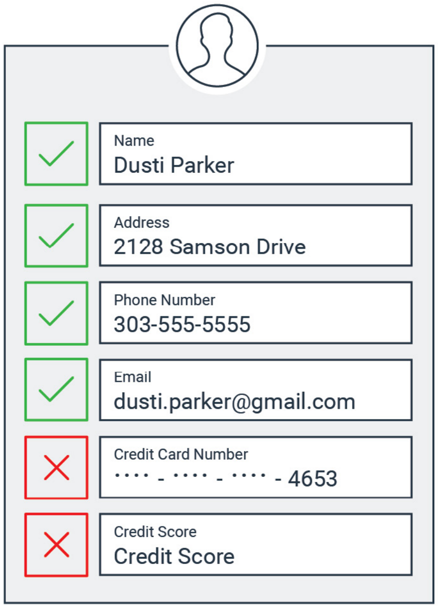
Support

If a customer requires support, it's often because they're experiencing a problem. If they're already a little frustrated, it becomes even more important to make their experience as painless and efficient as possible. For example, requiring them to go through a tedious process to identify themselves to a phone support rep after they've already logged in is NOT how you provide good support. It's also important to protect customer data and ensure that call center support reps don't have access to sensitive customer data that isn't required to do their jobs.

Objective: Resolve their problem quickly and efficiently, not add to their frustration

How identity addresses it:

- A face scan from a trusted device to verify customer identity
- Persistent sessions so a rep can ask "how are you?" instead of "who are you?"
- Delegated administration to control which user data support reps can see or edit



✓ Name
Dusti Parker

✓ Address
2128 Samson Drive

✓ Phone Number
303-555-5555

✓ Email
dusti.parker@gmail.com

✗ Credit Card Number
···· - ···· - ···· - 4653

✗ Credit Score
Credit Score

Customer identity can restrict customer service reps from seeing customer data they don't need to see.

Example: If your customer is logged into their account and uses the "call customer support" feature, they shouldn't have to provide their password again or remember the answers to security questions. Instead, their initial authentication should suffice. If they called into support directly, you could send a convenient push notification to their phone for authentication. You can also control what information from the customer profile is accessible by customer service reps, so you're able to protect sensitive data.

Personalization

Similar to self-service, personalization is about making customer profiles—user data, preferences and any other data you store—consistent no matter how your customer interacts with your brand. Personalization also allows you to leverage the preferences collected on other channels to cross-sell, promote and deliver better experiences on all channels.

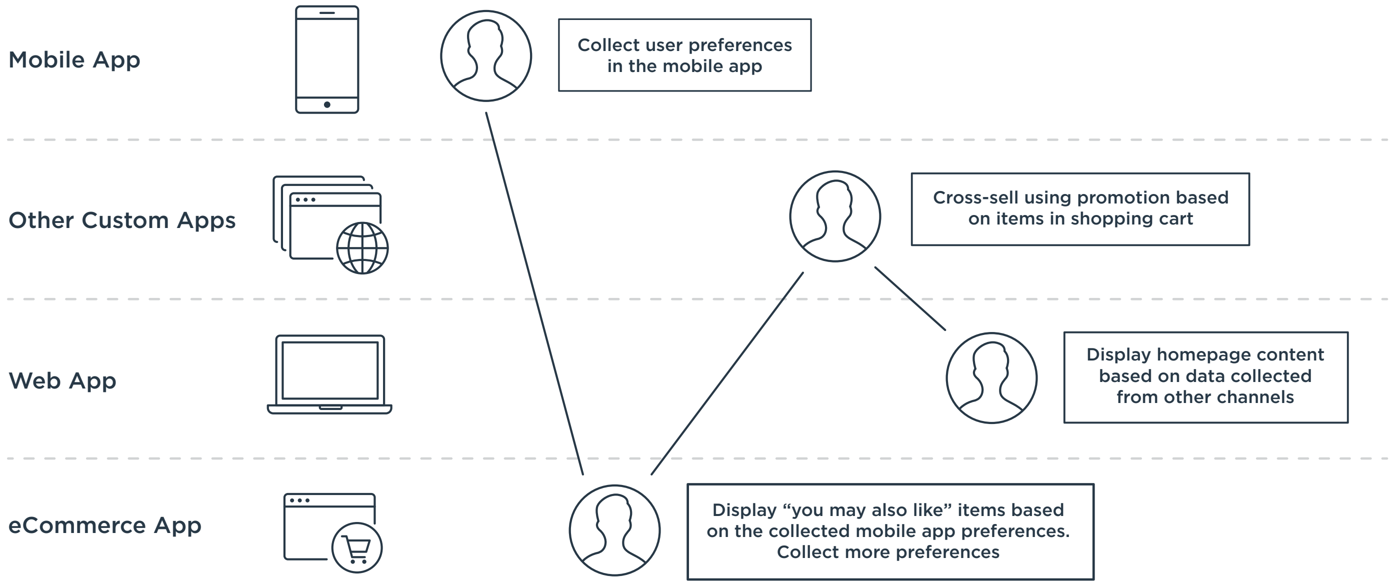
Objective: Deliver consistent multi-channel experiences

How identity addresses it:

- Consistent preferences across channels
- A unified customer profile that exposes the same customer profile and preferences to all apps
- Store any custom attributes and unstructured data your apps need in a customer profile
- Ability to consolidate unified profiles with bi-directional sync, migration and coexistence

Example: If a customer updates their preferences on your website to indicate that their hobbies include rock climbing, they should see helpful information or promotions related to rock climbing when they visit the mobile app, not promotions for something that isn't of interest.

Having a consistent view of customers across channels not only reduces disjointed, frustrating experiences, it also gives your business the opportunity to cross-sell and earn more revenue.


Mobile App
Collect user preferences in the mobile app
Other Custom Apps
Cross-sell using promotion based on items in shopping cart
Web App
Display homepage content based on data collected from other channels
eCommerce App
Display "you may also like" items based on the collected mobile app preferences. Collect more preferences

Having a consistent view of customers across channels not only reduces disjointed, frustrating experiences, it also gives your business the opportunity to cross-sell and earn more revenue.

Privacy

Privacy is a two-sided coin. On the one side, it allows you to comply with privacy regulations. But from the customer perspective, privacy is about giving them control over and insight into their data. Your customers should have the ability to make decisions about who their data is shared with, as well as what data is shared and how. They also need the ability to easily revoke consent at any time. Beyond merely collecting consent, though, you also need to enforce it. This is how you build trust.

Objective: Provide transparent privacy and consent management

How identity addresses it:

- Collection and storage of consent
- Enforcement of consent and privacy policies without requiring changes to your apps or APIs
- Transparency about how customer data is shared

Example: Many large enterprises have dozens of customer-facing applications. Instead of requiring each of them to update their requests for customer data to comply with customer consent, your customer identity solution should evaluate all requests against the rules set by your organization, then only return compliant customer data. By centralizing this capability, you don't have to audit the code of individual app teams to make sure their requests are compliant. In fact, app teams may not even know you've changed anything at all. After implementation, non-compliant data will simply stop being returned to them.

When enforcing consent and restricting data, it's important that your apps, consumers of data, as well as your APIs and user stores that store the data don't need to change. This makes consent much easier to audit.

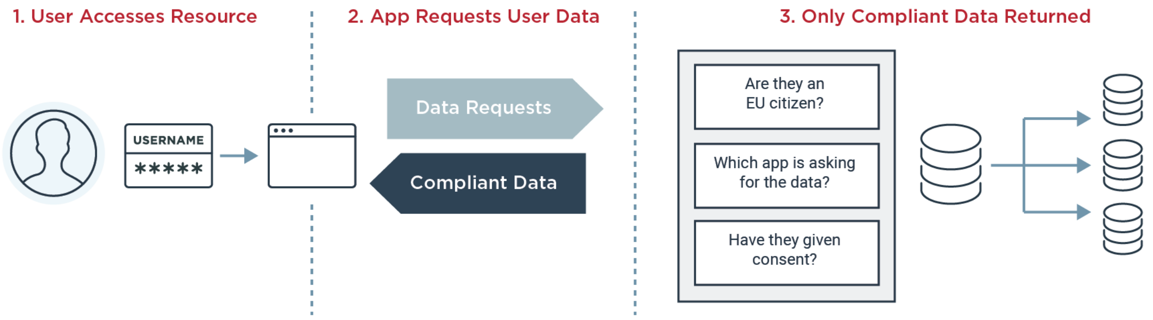
Regulatory Compliance: Challenge Meets Opportunity

Regulations like the EU's General Data Protection Regulation (GDPR) and Revised Payment Services Directive (PSD2), and the California Consumer Privacy Act (CCPA) are requiring organizations to evolve and adapt. To comply with the growing number of regulations, you need a foundation of privacy with the flexibility to build and enforce policies to meet both current and future requirements. Otherwise, you'll face the challenge of re-architecting each time a new regulation is introduced or a change is made to an existing one.

Because your ability to ensure data privacy is a core component of building trust and brand loyalty, the ability to provide self-service data privacy management can be a competitive differentiator. To build customer trust, you need to assure your customers that you're a good steward of their data. You can gain trust by making consent both easy and transparent, and giving customers full control over and insight into their data.

Data privacy management solutions help you comply with regulatory requirements, while also giving customers what they want by providing fine-grained data access based on real-time consent records.

Read the blog to learn more.


1. User Accesses Resource
USERNAME
*****
2. App Requests User Data
Data Requests
Compliant Data
3. Only Compliant Data Returned
Are they an EU citizen?
Which app is asking for the data?
Have they given consent?

When enforcing consent and restricting data, it's important that your apps, consumers of data, as well as your APIs and user stores that store the data don't need to change. This makes consent much easier to audit.

CHAPTER 04

EVALUATING CUSTOMER IDENTITY SOLUTIONS

As you evaluate the best customer identity solution for your needs, you may question if you need a dedicated customer IAM solution or if your current enterprise IAM solution can be extended to address customer requirements. Or you may wonder if you'd be better off building your own solution. To help you navigate, let's take a closer look at your options.

Option A: Extending Your Enterprise IAM Solution

As you consider how to address your customer identity needs, you may look first to your enterprise IAM stack. Since it may be working well enough for your workforce needs, you could be tempted to figure out how you can extend it to address your customer requirements as well.

If your requirements for customer IAM are minimal, your enterprise IAM solution may be up to the task. To evaluate if your current IAM stack is a feasible solution, you'll want to consider your requirements for scale, profile attributes and support.

- **Scale:** Do you need the ability to support spikes in demand? How many customer identities must you support? If you're supporting thousands of customer identities with no expectation of needing to support millions of identities in the future, and you can also expect a predictable volume of demand, your enterprise IAM solution may suffice.
- **Attributes:** Do you store a lot of different customer attributes? Do you need to support unstructured data or custom attributes? If your profile data consists of basic fields like name, email and address, you may be able to accommodate customer IAM with your enterprise stack. However, to provide customers with the best experience. you often need to store custom attributes like opt-ins or premium member status. You may even need to store unstructured data like a JSON blob of preferences or a browser fingerprint. Traditional IAM solutions may not be able to support these types of profile data and will limit the experience your applications can deliver to your customers.
- **Support:** Does your IT team have the ability to support app launches and tight deadlines? How many apps will IT need to support? By relying on your enterprise IAM stack, you'll also be relying on your current IT resources so you'll want to be sure you have sufficient resources to support the needs of fast-moving development teams.

It's possible you may find that your enterprise IAM solution is enough. But for many organizations, this evaluation will reveal many gaps. And it's no surprise, really.

Traditional IAM systems were designed for workforce applications where the main goal of the system was to protect enterprise data and manage internal access. Because these systems were built for non-customer applications and use cases, they aren't intended to accommodate critical customer features like self-service registration and account management, storing rich customer profiles, handling demand spikes, and many others.

Enterprise IAM also provides little regard for the experience customers demand. The features you consider to be optional nice-to-haves for your workforce are absolute must-haves for your customer use cases. Remember, unlike those in your workforce, your customers have a choice about interacting with you. Fail to delight them, and they won't hesitate to go to a competitor.

Bottom Line: Enterprise IAM Often Lacks Critical Capabilities for Customer Use Cases
Enterprise IAM may work for some less-demanding customer use cases. But for many, trying to extend enterprise IAM to address customer requirements creates unnecessary risks like:

- Poor customer experience
- No elasticity to accommodate spikes in engagement
- Limited horizontal scalability
- Increased security risks
- Regulatory compliance challenges
- No customer-friendly methods of multi-factor authentication

Read the blog to understand the advantages of storing customer and workforce identities separately.

Option B: Building Your Own Customer IAM Solution

Building your own customer IAM solution may seem like a smart way to meet your specific requirements, especially when you have developer resources in house. And you love a good challenge, right? But architecting a homegrown solution can be a massive undertaking that can slow down implementation.

It may seem that identity is little more than a registration and login form, but should you undertake building a customer identity solution, you'll soon find that there's much more than meets the eye. Other deliverables will soon become evident. You'll have to find answers to questions that can drastically slow down the time it takes to manage your identity solution and launch your applications like:

- How do you enable social registration and login?
- Are you prepared for the complexities of identity standards such as OAuth and OpenID Connect?
- How will you deliver SSO to custom—non-standards-based—apps?
- What about authentication policies for different apps?
- How will apps be protected from breach and fraud?
- What about MFA?
- How do you enforce privacy?
- Will customers be able to login during demand spikes?
- What about passwordless authentication?

If you have ready answers to these questions and ample resources to support a DIY system, then building your own customer IAM solution may be an option for you. But more likely, this exercise will produce a lengthy to-do list and illuminate the many disadvantages of trying to undertake a custom build and the maintenance required to support it.

Bottom Line: DIY Solutions Can Create More Problems Than They Solve
Instead of providing the customization you envisioned, building your own DIY solution for customer IAM often creates more problems like:

- Lengthy implementation
- Ongoing maintenance requiring specialized resources
- Potential security gaps
- Lack of standards support
- Inflexible project-specific solutions

Read the blog to better understand the risks of of building vs. buying a customer identity solution.

Option C: A Purpose-built Customer Identity Platform

Enterprise IAM just isn't a viable option for customer identity, and attempting to build your own solution is like trying to reinvent the wheel—or a supersonic jet. It just doesn't make sense to take on such a risky and overwhelming undertaking when you have the option of using an integrated customer identity platform instead.

A purpose-built platform solution that's designed specifically for the requirements of customer identity and developed by identity experts—who've spent decades getting it right—gives you all of the capabilities you need to deliver the seamless and secure CX your customers want. You're able to:

- Give your customers easy-to-use registration, sign-on and more so you can acquire more customers and keep them coming back
- Deliver personalized, multi-channel experiences that drive revenue wherever customers interact with your brand
- Give customers full control over and insight into their data to adhere to privacy regulations and build trust

Bottom Line: A Purpose-built Customer Identity Platform Provides Everything You Need
A fully integrated customer identity platform provides powerful capabilities like:

- Enterprise-grade authentication for single sign-on
- Adaptive multi-factor authentication with support for multiple authentication options, including passwordless
- Configuration and customization options to deliver personalized experiences
- Ability to store identity and profile data how and where you'd like
- Regulatory compliance and consent management
- Handle complex enterprise use cases with custom apps
- Meet scale and security SLAs

To see what KuppingerCole analysts recommend you prioritize in a customer identity solution, get the report.

	Build CIAM Yourself	Enterprise CIAM	Purpose-built CIAM
Scale/Perfornance	Possible, but requires specific expertise and resources to manage	May not meet CIAM scale/ performance requirements	Built to handle and adapt to changing CIAM scale and performance needs
Security	Possible, but requires specific expertise and resources to manage	May not meet enterprise CIAM security SLAs	Provides built-in security (particularly in enterprise-focused CIAM solutions)
Resources Required	Requires specialized, technical resources to build and maintain	Requires IT resources to support app teams	Resource requirements needed primarily for deployment
Time	Slow	Slow/Medium	Fast
Customer Data	Can architect the identity data store however you like	May have rigid schema and limit what type of customer data you can store	Flexible schema to store custom and unstructured attributes
MFA	Possible, but time-consuming to build	May not have customer-friendly authentication factors (e.g., push notifications from custom apps)	Many will have focus on customer-friendly authentication factors
Authentication	Resources required to build SSO use cases, passwordless, social login/ registration, adaptive policies and other use cases	Most CIAM features not available	Provides out-of-the-box passwordless, adaptive authn, social registration/ login, and other CIAM capabilities
Customer Experience	You will have complete control over the experiences you build	Experiences may be less than optimal for customers	Templates and APIs to make customer experiences match your brand

CHAPTER 05

START BUILDING YOUR BUSINESS CASE FOR CUSTOMER IDENTITY

CX is a strategic priority for many organizations. A thoughtfully chosen and well-implemented customer identity solution can make a huge impact on both your organization's top and bottom lines. Yes, many are challenged to demonstrate the return on investment that CX (and by proxy customer identity) provides.

According to Gartner's 2019 Customer Experience Innovation Survey, "Many organizations have faced crisis situations in their CX program within the last three years. Economic or financial pressure has impacted the highest proportion of respondents (53%). For those with lower maturity levels, 60% had CX initiative launches stalled due to lack of executive support, and 59% found it difficult to demonstrate value or ROI, which leads the CFO to question all future investments."

While the ultimate decision maker in your organization may vary, it's not unusual for line-of-business (LOB) executives as well as IT executives to be involved. It behooves you to involve these LOBstakeholders because they have access to larger budgets and can help you evangelize the benefits of customer IAM when you demonstrate its value. Because customer identity data is of interest to marketing and sales, you'll also want to consider their needs to ensure you identify the right solution to meet cross-functional requirements.

Building a business case for a customer identity starts with recognizing and understanding that customer IAM has a broad impact on your organization. Ensuring you address individual interests is key to making a business case and the best decision. Here are the typical players involved and how to appeal to what they care about most.

Business Executives

Business executives are focused on the overall business and decisions that will advance big-picture objectives. That means you want to avoid talking about details like login forms and profile management. Instead, start with an understanding of what their goals are, then convey how customer identity aligns to them. Focus your message on how identity helps you deliver better customer experiences that ultimately drive revenue. Highlight that identity can help you significantly reduce abandonment, acquire customers, and increase engagement. Remember, these are the people who have access to large budgets, so making a case for how customer identity can advance your organization's strategic objectives can move the needle in a big way for your organization.

What They Care About: How customer identity impacts top-line revenue, customer acquisition and retention.

How to Communicate Customer Identity's Value:

- Build support by providing an analysis of the business value customer identity creates, measured in revenue, customer acquisition, and similar metrics
- Share data on current abandonment rates for login and registration forms and explain how identity can improve them
- Provide specific examples of how customer identity can improve CX (we've provided several throughout this guide)

IT Executives

IT leaders may be tuned into customer experience and revenue to some degree, but they're also burdened by taking on more responsibility and with fewer resources. They're concerned about how a solution is architected and how well it can adapt to meet changing requirements. You'll want to address how it can reduce costs, improve business agility and ensure security.

What They Care About: How customer identity meets their needs and impacts bottom-line savings.

How to Communicate Customer Identity's Value:

- Discuss the ways that customer identity makes IT more efficient
- Demonstrate how it offers a lower total cost of ownership (TCO)
- Address the need for scale and adaptability and how customer identity meets it
- Identify your various customer use cases and how customer identity supports them
- Address the need for security and how customer identity meets it

IT / IAM Professionals

These IT or identity experts are the ones who have to get their hands dirty implementing whichever solution is chosen. As a result, they'll be concerned with the capabilities of the solution and whether it's going to be able to meet their needs and address the specific use cases within their enterprise.

What They Care About: What capabilities customer identity provides and how easy it will be to implement and manage.

How to Communicate Customer Identity's Value:

- Focus on core capabilities, like policies, MFA and passwordless
- Provide access to technical specifications and details

Security Teams

What keeps security teams up at night is worrying about resources being secure and risks being managed effectively. A breach is their worst nightmare. Their mission is to ask the tough questions to reveal the vulnerabilities.

What They Care About: How customer identity helps secure resources and minimizes risk.

How to Communicate Customer Identity's Value:

- Address how it helps alleviate security demands
- Highlight capabilities like MFA, data encryption and support for open standards

Application Teams

App teams have one goal above all others: Launch apps on time. Often, app developers aren't identity or security experts, so these processes can slow them down. Identity can help app teams by taking the complexities of identity and security off their plates and ensuring that they can focus on the app's features and meeting critical app launch deadlines.

What They Care About: How customer identity helps them go to market quickly.

How to Communicate Customer Identity's Value

- Focus on speed and efficiency of getting customer IAM into their apps

To learn more about collaborating on customer identity with others in your organization, get the quick guide.

Getting Customer Identity Right

CX is still the battlefield on which brands compete. Those who prioritize delivering extraordinary CX will emerge as the leaders in their industries and categories.

By using customer identity to address your customers' expectations throughout their journey, you're on your way to delivering the standout CX that will position you for competitive advantage. When you get customer identity right, you're able to:

- Acquire and retain more customers
- Drive revenue and loyalty
- Build customer trust

Providing frictionless registration and sign-on is step one. Ping Customer360 helps you make the strong first impression needed to get more customers and keep them coming back for more.

To learn more about using customer identity to deliver extraordinary experiences, visit our website.

Ping Identity is pioneering Intelligent Identity. We help enterprises achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The Ping Intelligent Identity™ platform provides customers, employees, partners and, increasingly, IoT, with access to cloud, mobile, SaaS and on-premises applications and APIs, while also managing identity and profile data at scale.

#3146 | 12.20 | v02