

When we think about identity design, security teams are often front and center — and understandably so. After all, safeguarding user accounts is critical in today's interconnected digital world. However, effective identity design is not a solo act by security experts. To create seamless, trustworthy, and user-friendly identity experiences, a diverse range of teams must come together, from product to privacy and customer support.

Companies like **Arena Plus**, **Houzz**, and **Houzz Pro** understand this well. They've embraced an inclusive approach that goes beyond just technical controls to craft reliable identity flows that balance security, usability, and privacy. Let's dive into who else needs to be involved in identity design and why.

Beyond Login: The Digital Identity Lifecycle

Too often, identity design conversations zero in on login and password screens. While these touchpoints are crucial, identity spans a user's entire lifecycle:

- **Registration:** The very first impression where simplicity and clarity reduce friction.
- **Authentication:** Access methods including passwordless options that enhance security while maintaining ease of use.
- **Authorization and Risk Management:** Step-up checks and risk-based authentication to keep suspicious logins at bay without frustrating legitimate users.
- **Account Recovery:** Supportive yet secure recoveries to regain access without unnecessary delays.
- **Ongoing User Management and Privacy:** Transparent settings that empower users to control their data and permissions.

As you can imagine, each stage requires input from different expertise areas.

The Product Team: Advocates for User Experience

The product team is responsible for the overall user journey and experience. Their involvement ensures that identity flows are intuitive and aligned with broader product goals. Here's what they bring to the table:

- **Clear, Minimal Registration Fields:** The product team prioritizes simplifying registration forms. For example, Arena Plus has streamlined signup by minimizing mandatory fields, reducing drop-off rates significantly.
- **Consistent Terminology:** They ensure language is consistent between registration, login, and recovery flows. A common pet peeve in identity design is inconsistent terms—for example, "sign up" versus "register" or "reset password" versus "recover account." These inconsistencies confuse users and increase support load.
- **Seamless Passwordless Access:** Collaboration with security and UX to introduce modern options like **passkeys** and **fingerprint authentication**. Houzz Pro has successfully reduced password fatigue by adopting fingerprint authentication on its mobile app, making access quick and secure.
- **Balancing Friction and Security:** Product teams advocate for risk-based authentication flows that challenge users only when necessary, enhancing security without causing frustration.
- **Data Collection Ethics:** They keep an eye on avoiding unnecessary data collection, helping maintain trust and compliance with privacy standards.

The Privacy Team: Guardians of User Data

Privacy teams are critical partners in identity design, especially as regulations tighten worldwide. Their involvement ensures identity solutions respect user data rights and meet legal obligations.

- **Minimizing Data Exposure:** They work with product and security teams to collect only what's necessary during registration and authentication.
- **Transparency and Consent:** They help craft consent prompts that are clear and not misleading. Permission requests—especially for biometric data—must never be preselected; users should make explicit choices.
- **Privacy by Design:** Privacy teams advocate that identity designs include privacy considerations from the start, not as an afterthought.
- **Clear Communication:** Collaborate on explaining how biometric options like fingerprint authentication are handled, stored, and used, keeping users informed and reassured.
- **Support for User Rights:** Facilitating easy access to data correction, deletion, and export falls under their purview.

For example, Houzz includes privacy notices clearly linked during sign-up and when enabling biometrics, respecting users' need to make informed decisions without clutter or confusion.

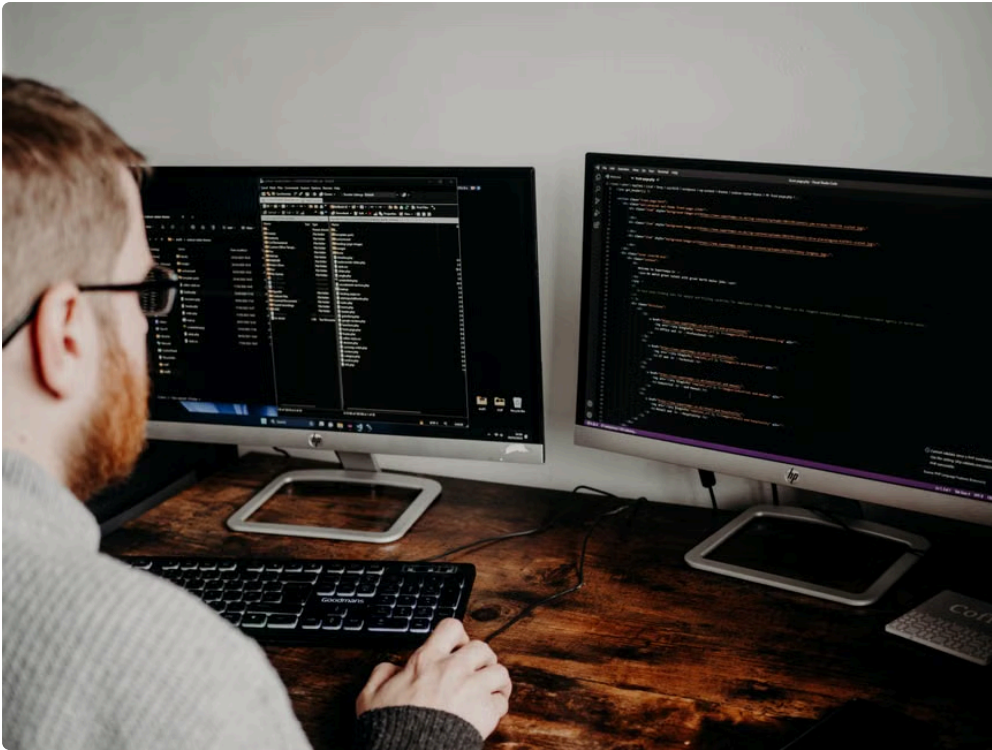


Customer Support: The Frontline Problem Solvers

Customer support teams have direct contact with users encountering problems in the identity flows. Their insights are invaluable:

- **Understanding Common Pain Points:** Support teams identify where users struggle—be it confusing error messages or account recovery hurdles.
- **Consistent Messaging:** They ensure internal support language aligns with external user messages to avoid mixed signals.
- **Security Awareness:** Support must be trained on what they should *never* ask for, such as passwords, recovery codes, or passkeys, to avoid phishing risks. This list should be regularly updated and enforced.
- **Clear Guidance on Recovery Processes:** Support teams help users navigate risk-based step-up authentications and verify identities without frustration.

Arena Plus, for instance, routinely compiles [passwordless login](#) user queries related to identity issues and works with product and security teams to adjust flows accordingly. This collaborative feedback loop improves usability and trust.



Security Teams: The Essential Protectors

While this blog focuses on teams beyond security, it's worth mentioning their ongoing role:

- **Risk Monitoring:** Implementing risk-based authentication that steps up verification dynamically based on contextual signals — device reputation, geolocation anomalies, or unusual behavior.
- **Integrating Modern Authentication Methods:** Driving adoption of passwordless options like **passkeys**, reducing reliance on passwords that are prone to phishing.
- **Keeping Up with Threat Landscape:** Updating identity defenses continuously to mitigate emerging threats.
- **Technical Verification:** Ensuring the cryptographic security behind biometric and passwordless methods is sound.

They are indispensable, but their success depends on collaboration with supporting teams.

Key Considerations for a Winning Identity Design

Focus Area Who's Involved Best Practices Registration Product, Privacy Minimal fields, clear language, privacy notices upfront Authentication Product, Security, Privacy Passwordless methods (passkeys, fingerprint authentication), risk-based step-up Account Recovery Support, Product, Security Clear recovery options, prevent support asks for sensitive info User Privacy & Data Privacy, Product Consent management, data minimization, transparency Ongoing Support & Messaging Support, Product Consistent terminology, clear error messages, user education

Avoiding Common Mistakes

One common mistake with identity design content is the omission of transparent information regarding costs. Many companies scrape or recycle help docs without including pricing, fees, or promo amounts related to identity features or support services. It's crucial never to invent or speculate on costs. Instead, always communicate pricing specifics explicitly if applicable or clearly state when no fees are associated.

Transparency builds trust, and withholding or confusing pricing details harms user confidence and satisfaction.

Conclusion

Effective identity design is a team sport. Beyond security teams, the product team shapes smooth, user-friendly experiences; privacy teams uphold trust and legal compliance; and customer support bridges the gap between technology and human interaction. Together, they create identity flows that are secure, private, and seamless.

Companies like Arena Plus, Houzz, and Houzz Pro show the benefits of this collaborative approach — offering users state-of-the-art passwordless options such as passkeys and fingerprint authentication, minimal registration friction, and thoughtful risk-based authentication.

If your organization hasn't yet embraced a wider team perspective on identity design, now is the time. Secure accounts alone aren't enough; users expect identity journeys that respect their privacy, help them swiftly recover access, and empower them to engage with your product confidently.