

We Need to Rethink Our Approach to Customer Data and Identity Verification. Here's Where to Start.

Opinions expressed by Entrepreneur contributors are their own.

Key Takeaways

- Online identity must shift from storing customer data to requesting verifiable proofs.
- zkTLS turns verification into a yes or no proof, not a document upload, which ties back to the goal of proof over storage.
- Using proof over storage reduces compliance risk and accelerates decisions without expanding the data you hold. It's safer and more respectful of users' privacy.

Online identity should move from storing data to verifying proofs. The internet already holds what onboarding and risk teams need, from degrees and loyalty tiers to proofs of payment. The challenge is verifying these facts reliably without compromising privacy. That is why the secure layer of the internet, TLS, needs a zero-knowledge twist so verification happens without hoarding data.

For founders, every onboarding form, fraud check and compliance workflow is a balancing act; verify users without turning into a data honeypot. The internet already holds what businesses need – from proof of education to proof of purchase – but the real challenge is verifying those facts without

storing or leaking sensitive information. So, what if verification didn't require storage at all?

Related: [How to Master the 5 Primary Challenges in Online Verification](#)

Closing the trust gap

Data breaches are costly, with IBM estimating the 2025 global average at about \$4.4 million. Automation is amplifying threats, and malicious bots account for roughly 37% of internet traffic.

This transformation is happening in tandem with shifting privacy expectations, as a 2025 investigation found over 30 data brokers hiding opt-out and deletion pages from search, drawing federal pressure and state scrutiny, while California's privacy regulator advanced a unified deletion mechanism called DROP under the Delete Act. This reinforces the shift from storing customer data to requesting verifiable proofs. For founders, this shift means less liability and faster compliance, but only if verification methods evolve with it.

zkTLS simplified

Whenever a user logs into a secure website, a "TLS handshake" is orchestrated by the browser and the website. What Zero-Knowledge Transport Layer Security (zkTLS) does is enable the generation of a cryptographic proof through this session, a proof that states a specific, factual occurrence that took place on the site, without revealing the page or underlying data. This translates into verifying data without having to store a document that reveals the data to be verified.

This eliminates the need for password sharing, and it is by no means screen scraping, as the evidence is derived from the

session itself. A multitude of implementations utilize a witness or proxy model that attests access to the domain and content, producing verifiable proof.

This turns verification into a yes or no proof anchored to a real TLS session, not a document upload, which ties back to the goal of proof over storage.

The difference it makes

In short, proof over storage reduces risk and speeds decisions without expanding the data you hold. zkTLS provides the assurance of verification while minimizing the attack surface. All that's requested is the minimum proof required, meaning fewer honeypots, simplicity in reviews and a much faster user experience. This also maintains humanity in incentives and communities, as proofs are bound to a durable identity while protecting the privacy of personal information.

It's not just safer, it's more respectful of users' privacy. Instead of storing identities, you verify them – and move on.

Related: [How Blockchain's Decentralization Narrative Can Redefine Data Privacy](#)

zkTLS in practice

Humanity Protocol uses zkTLS to turn Web2 facts into reusable proofs that apps can verify without ever seeing the underlying page. When visiting a trusted site, users generate proof of a specific claim, with the claim attached to their "Human ID," which can then be verified by apps while maintaining the privacy of the underlying page and irrelevant data. This has been scaled across employment, education and travel loyalty. It replaces document collection with minimal proof that answers only the question at hand.

Business cases you can ship this quarter

If your business policy has a specific threshold, you can establish proof of the threshold. For instance, decline “balance below X” instead of gathering full statements, thereby reducing backlogs, lowering data retention risk and fast-tracking the onboarding process through this selective disclosure. Another interesting use case is loyalty status, where users can confirm their status without sharing their data, unlocking seamless sign-in experiences without the daunting manual processes of yesteryear.

This is made resilient by sybil-resistant growth loops that verify through human reputation rather than personally identifiable information (PII), as proof of humanity is paired with anomaly detection as a countermeasure to automated abuse.

Lastly, zkTLS can verify employment and verification in a matter of minutes through proofs from official portals, avoiding the perpetual ping-pong of emails and documents, and maintaining focus on candidates rather than paperwork. Each claim replaces a document, cutting storage risk and speeding decisions.

What implementation would look like

Businesses must start by identifying a particular claim that can develop trust or minimize funnel cost while outlining definable success metrics, whether conversion lift or reduction of review time.

With the claim identified, it's crucial to be selective in required disclosures, whereby excess data is treated as a liability. This must be built on a familiar user experience on sites that users already utilize, with consent forms to generate proof in their browsers, showcasing what will be

checked and what will never be seen.

While developing this methodology, it's crucial to maintain fallback methods for those who can't generate proofs, such as manual reviews. The verified attributes could then be reused across a multitude of product lines, and as businesses scale, across partner ecosystems, creating portability that compounds trust and minimizes repeated friction for customers.

Related: [The Future of Identity Verification](#)

Risk, compliance and governance

The lesser the data held by companies, the smaller the blast radius in case of incidents. This is where the industry advises minimal data collection and storage, highlighting that the complication or hiding of deletion and opt-out choices is under active 2025 scrutiny, and California's DROP system will centralize broker deletions. Businesses must anchor their programs to transparency of consent and convenience in revocation.

The evolution of online identity won't be in the size of databases, but in proof. zkTLS translates trust signals in Web2 into portability in privacy-first credentials that are controlled by customers and verified by systems. The key to this methodology is starting with one attribute, measuring its impact and exploring how it can be scaled.

Key Takeaways

- Online identity must shift from storing customer data to requesting verifiable proofs.
- zkTLS turns verification into a yes or no proof, not a document upload, which ties back to the goal of proof over storage.
- Using proof over storage reduces compliance risk and

accelerates decisions without expanding the data you hold. It's safer and more respectful of users' privacy.

Online identity should move from storing data to verifying proofs. The internet already holds what onboarding and risk teams need, from degrees and loyalty tiers to proofs of payment. The challenge is verifying these facts reliably without compromising privacy. That is why the secure layer of the internet, TLS, needs a zero-knowledge twist so verification happens without hoarding data.

For founders, every onboarding form, fraud check and compliance workflow is a balancing act; verify users without turning into a data honeypot. The internet already holds what businesses need – from proof of education to proof of purchase – but the real challenge is verifying those facts without storing or leaking sensitive information. So, what if verification didn't require storage at all?

The rest of this article is locked.

Join Entrepreneur+ today for access.

<https://www.entrepreneur.com/science-technology/why-its-time-to-rethink-customer-data-collection/497707>