



THE SHOT PAPERS

PROOF OF HUMAN.

What sport knows that the internet forgot. The web can no longer tell people from software, and every fix on the table asks you to pay with your body, your documents or your privacy. Sport has been running a better verification system for a century: the register, the touchline, the Tuesday night. This paper is about what that is worth, and how we built it into an identity a person can carry for life.

FOR FEDERATIONS · BRANDS · IDENTITY AND TECHNOLOGY LEADERS

SHOT Clubhouse Limited · Company no. 16350767 · 86-90 Paul Street, London EC2A 4NE

shotclubhouse.com



THE ARGUMENT IN ONE PAGE

More than half of the traffic on the web is no longer human, and the internet has no reliable way to tell the difference. Every serious answer so far asks people to hand over their bodies, their documents or their behaviour. Sport already solved this problem, and nobody noticed, because sport never called it verification. It called it turning up.

SIX FINDINGS

1. **The bots hold the majority.** Automated traffic passed half of all web traffic in 2024, at 51%, and malicious bots alone accounted for roughly 40% by the 2026 report. Those figures come from one security vendor's telemetry, so treat the decimals with caution; the direction is not in doubt.
2. **The people building AI agree there is a problem.** In 2024, 32 researchers spanning OpenAI, Microsoft, Harvard and MIT published a paper calling for "personhood credentials", privacy-preserving proof of who is real online. It is a preprint, not peer-reviewed, but the authorship is the point: the builders of the machines are asking for a way to tell people from their own products.
3. **The current fixes fail in three different ways.** Biometric proof-of-human asks you to trade your body for access. Behavioural detection is losing an arms race to AI. Platform verification badges are bought, not earned.
4. **Sport already verifies humans.** Continuously, in person, for free, witnessed by a community, on a weekly schedule, and it has done so for over a century. It is one of the last institutions on earth that still does.
5. **The principle is proof-of-active-personhood.** Verified once. Attested by your culture. Recharged by participation. Your body is not your password; your Tuesday nights are.
6. **The design intent is clear.** Sport Head ID is being designed around a participation graph signed by real coaches and clubs, a live activity signal called Charge, minimum data capture, selective disclosure, and a credential controlled by the person. The aim is to minimise data, avoid profiling within the identity layer and keep identity from becoming the product. Those are principles against which the implementation should be judged, not a claim that every part is final today.

A bot can fake a face better every year. It cannot turn up to training on a wet Tuesday in February, be seen by thirty people who know it, and do it again every week for a season.

The rest of this paper walks through the evidence, the failures of the current answers, the principle any institution could adopt, and the specific way we are designing it.

1 THE COACH WHO TURNS UP EVERY TUESDAY

I ran a grassroots girls' football club that grew from five players to hundreds of kids a week, and the thing that made it work was not talent or money. It was the volunteers who turned up every Tuesday.

Think about one of them. A fellow volunteer coach, a parent who got roped in like most of them do. Every Tuesday night, in daylight and in drizzle, he was on that pitch. He signed the register. He set out the cones. Forty parents on the touchline could pick him out of a crowd. The kids knew his voice before they saw him. The club secretary held his safeguarding certificate in a drawer. The league had his name on a team sheet every weekend. If he had stopped coming, we would have known by the second Tuesday, and someone would have rung him to ask if he was alright.

Now ask what any online platform knows about its most engaged user. An email address that might be disposable. A date of birth typed into a box. A pattern of clicks that a piece of software can now imitate perfectly. The platform cannot tell you whether its user is a person, let alone whether that person is well, or present, or real in any way that matters.

The club knew all of it without collecting a single database field. The knowledge was held in the community itself: repeated, in-person, witnessed presence over time. Nobody designed it as a verification system. It is simply what a sports club is.

Sport does this for everyone it touches, not just coaches. The player whose attendance is marked every session. The parent on the same patch of touchline every week. The referee, the fixtures secretary, the teenager who helps pack the goals away. Sport verifies humans continuously, in person, for free, witnessed by a community, and it has done so since before anyone thought to call it verification. The pub used to do it. The church used to do it. The workplace did it until work went remote. One by one those institutions have thinned out or moved onto screens. Sport still gathers real people, in real places, on a schedule, every week of the season. It is one of the last institutions on earth that does.

The most valuable identity infrastructure in the world is already running. It meets on Tuesday nights.

2 THE PROBLEM IN NUMBERS

In 2024 the internet crossed a line most people never noticed: for the first time, the majority of web traffic was not human.



Start with the traffic. According to one large security vendor's telemetry across its own network, automated traffic reached 51% of all web traffic in 2024, and malicious bots alone climbed to roughly 40% of everything by its 2026 report, with AI agent traffic growing many times over year on year. These are one company's measurements, not a census of the internet, so hold the decimal points loosely. The direction of travel is not seriously contested by anyone who runs infrastructure: the human share of the internet is shrinking, and the software share is accelerating.

The people building the AI can see it. In August 2024, 32 researchers whose affiliations spanned OpenAI, Microsoft, Harvard and MIT published a paper arguing for "personhood credentials": privacy-preserving credentials that let a person prove they are real online without revealing who they are. It is a preprint and has not been peer-reviewed, so I cite it as a signal rather than settled science. But read the author list again. The organisations releasing the most capable AI systems in history put their names to a paper saying the internet will soon need a way to distinguish people from their products.

The market has noticed too. The best-funded consumer answer so far is an iris-scanning proof-of-human project that verifies people by photographing their eyes with a custom orb. By April 2026 it was announcing integrations with mainstream dating, video-calling and document-signing apps, moving from crypto curiosity to consumer plumbing. Over the same period it has been banned or suspended in several jurisdictions over biometric data concerns, and critics point out two things that do not go away: an iris cannot be reissued if the data is compromised, and paying people to scan their eyes lands hardest on the people who most need the money. Both halves of that story are true at once, and any honest account of this market has to hold them together.

Meanwhile the compliance economy grows underneath it all. One analyst house puts the age assurance market at \$5.7 billion in 2025, projected to reach \$10.4 billion by 2029; estimates of the broader identity verification market for 2026 run in the tens of billions, with growth forecasts in the mid to high teens. These are analyst projections, so I give them as a range, not a fact. The point is not the precision. The point is that "prove you are a real person" has become one of the fastest growing industries on earth, and almost every product in it starts from the same assumption: that the only way to prove you are human is to hand something over.

3 WHY THE CURRENT ANSWERS FAIL

Three families of fixes dominate the market. Each fails for its own reason, and all three share a deeper flaw.

BIOMETRICS: YOUR BODY AS THE PRICE OF ENTRY

Iris scans, face maps and fingerprints prove something real: that a living human was present at the moment of enrolment. The cost is the trade. You hand over the one credential you can never change. A password can be reset and a document can be reissued; an iris cannot. That is why several jurisdictions have banned or suspended the leading iris-scanning project, and why the practice of paying people, disproportionately in poorer countries, to scan their eyes draws the criticism it does. And even where the trade is accepted, a biometric check answers the wrong question. It proves you were a human once, at a kiosk. It says nothing about whether the account trading on that proof six months later is still you, still active, or still anything at all. Verified accounts get sold. The scan does not follow the life.

BEHAVIOURAL DETECTION: AN ARMS RACE THE HUMANS LOSE

The second family watches how you behave: how you move a mouse, how quickly you type, whether you can find the traffic lights in a grid of photographs. This worked while software was clumsy. It is not clumsy any more. Modern AI passes the tests designed to catch it, often more reliably than the people the tests were built to protect, and every escalation adds friction for real humans while the bots route round it. A detection system that trains against AI output is in an arms race with an opponent whose training budget is measured in billions. The trajectory only points one way.

PLATFORM BADGES: VERIFICATION AS A PRODUCT

The third family is the verification badge. The tick once meant a platform had checked who you were. On several of the world's largest platforms it now means a card on file: verification became a subscription line, and the badge measures willingness to pay, not personhood. A signal that can be bought is not a signal; it is a price.

THE SHARED FLAW

All three approaches ask a stranger to prove themselves to a machine, once. None of them can answer the question that actually matters to a community, a federation or a brand: is this a real person, living a real life, active right now? A snapshot cannot answer that. Only continuous, witnessed presence can, and machines do not witness. Communities do.

Every current fix verifies a moment. The thing worth verifying is a life.

4 THE PRINCIPLE: PROOF-OF-ACTIVE-PERSONHOOD

The alternative is not a better scan. It is a different question. Not "can you prove you are human?" but "can your culture vouch that you are living a human life in it?" I call the answer proof-of-active-personhood, and it rests on three properties.

1

VERIFIED ONCE

A person establishes who they are one time, at a level appropriate to what they do. A player needs less than a coach; a coach needs less than someone handling money. Verification is a rung you climb when a role demands it, not a toll gate at the door, and never a reason to surveil anyone afterwards.

2

ATTESTED BY YOUR CULTURE

The people who share your real life sign small, dated notes about it. The coach who ran the session. The club that hosted the fixture. The event you checked into. Each note is witnessed in person and signed by both sides, and over the years they accumulate into a web of vouches no stranger and no machine could fabricate.

3

RECHARGED BY PARTICIPATION

The proof is alive. It fades if you stop showing up and recharges when you return, so it always answers the present-tense question: is this person active in the culture now? A snapshot proves a moment. A recharging signal proves a life.

Notice what this principle does not require. No iris. No fingerprint. No real name shouted to the world. No behavioural spying. The evidence is the participation itself, witnessed by people who were there, and the person carries the proof rather than the platform owning it.

Notice also that the principle is not ours to fence off. Any institution with scheduled, in-person, witnessed participation could implement it: a choir, a cadet unit, a park run, a volunteer fire service. I would genuinely welcome that. Sport happens to be the natural home because it is the largest and most global version of the pattern, it already runs on registers and fixtures and checked adults, and it repeats weekly for most of the year across every country on earth.

And the honest limits, stated plainly: attestation can be gamed by collusion, so the design has to make collusion expensive, with both parties signing, limits on how much any one voucher can contribute, and revocation that costs the cheat rather than the victim. Proof-of-active-personhood also does not replace a document check where the law requires one. It sits alongside, and answers the one question the document never can.

Your body is not your password. Your Tuesday nights are.

5 THE BUILD: SPORT HEAD ID

We are building proof-of-active-personhood into a credential called the Sport Head ID. The design intent is that control sits with the person, and the implementation should be judged against that standard.

A PARTICIPATION GRAPH DESIGNED TO RESIST BACKFILLING

The proposed core of the credential is a graph of signed attestations from real coaches, clubs and events: the coach signs that the session happened, the player co-signs, and neither side should be able to fabricate the note alone. Each attestation would be a dated cryptographic record of a moment that has passed, designed to make backfilling difficult and visible. A click farm can create a million accounts tonight. The model is intended to stop it inventing a Tuesday from last March.

CHARGE: THE INTENDED LIVE SIGNAL

From that graph the design computes Charge, a live activity signal. Recent participation would count for more than old participation; the signal would fade if someone stopped showing up and recharge when they returned. The person should always be able to see their own Charge and what feeds it. The goal is a credential that is harder to fake than a snapshot because holding it requires repeated, witnessed participation over time.

MINIMUM DATA CAPTURE

The ID is being designed to start with the least information needed, not the most that could be collected. A real name is not intended to be required at entry, and the identity layer is not being designed as a marketing profile. Stronger verification belongs higher on the ladder, where a role demands it: coaching children, holding a federation office, handling money. For everyone else, the design aims to stay light.

SELECTIVE DISCLOSURE

The credential is being designed to reveal only what the checker needs. The aim is to let someone prove an age band without revealing a birthday, or recent activity without revealing where, with whom, or on which days. The verifier should get the answer to its question and nothing else.

OWNED FOR LIFE

The intention is that the person can keep control of the credential wherever they go: between clubs, sports, countries and apps. Open standards are the route to making it independently checkable and portable rather than dependent on one platform. If a better app comes along, the design should allow the person to move without leaving their identity behind.

The intent, plainly: identity should not be the product. The ID is being designed to minimise data, avoid profiling within the identity layer and give the person control over what is disclosed. That is the standard the implementation should be judged against as the model develops.



TAKE YOUR SHOT

Sport spent a century building the world's best human verification system without meaning to. We are turning that idea into a credential designed around the person. Here is what I am asking of each reader.

Federations. Your registers, your events and your coaches are the trust layer this whole model depends on. Issuing against a portable credential could make records independently checkable without surrendering members, data or commercial relationships. Bring us your hardest tournament check-in problem and help us test what an attested member should look like in practice.

Brands. Stop paying to reach accounts and start asking how to reach verified active humans. A release gated on witnessed participation should be harder to bot-farm because the qualifying signal is earned on grass, in gyms and in halls over months, not clicked in a second. If your last drop was won by scripts, help us pressure-test what a participation-gated one could look like.

Identity and technology leaders. The proposed implementation uses open standards: verifiable credentials, selective disclosure and transparency logs. The primitives are available to inspect and the model is there to challenge. Come and pressure-test it; the hard questions make the credential better.

And if you take one idea from this paper, take the principle rather than the product. The internet is about to spend billions asking people to prove they are human with their bodies. Sport has been proving it with presence, witnessed by a community, for over a century. Build on that, with us or without us.

Take your SHOT. Own it. Make impact. · shotclubhouse.com

SOURCES

- Imperva Bad Bot Report 2025 and 2026 (automated traffic 51% in 2024; malicious bots rising from 37% to roughly 40% between the 2025 and 2026 reports; AI agent traffic growth). Vendor telemetry from a single security provider, flagged as such in the text.
- "Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online", 32 authors with affiliations including OpenAI, Microsoft, Harvard and MIT, arXiv:2408.07892, August 2024. Preprint, not peer-reviewed. Explainer: MIT Technology Review, September 2024.
- Industry reporting on an iris-scanning proof-of-human project: consumer app integrations announced April 2026 (CoinDesk); bans, suspensions and biometric criticisms in several jurisdictions (The Conversation; Rest of World).
- Liminal, age assurance market estimates: \$5.7bn (2025) projected to \$10.4bn by 2029. Analyst estimate.
- Identity verification market estimates for 2026 and beyond (Fortune Business Insights and other analyst houses). Cited as a range of analyst projections only.
- Ofcom / UK Government, Online Safety Act age-assurance duties enforceable from July 2025, with initial fines issued.
- Australian Government Age Assurance Technology Trial, final report, September 2025 (age assurance technically feasible; no single solution fits all).
- W3C Verifiable Credentials, selective disclosure formats and Certificate Transparency: the open standards families referenced in Part Five.

The coaching story in Part One is drawn from my own years running a grassroots girls' football club; the fellow volunteer is anonymised and described with his knowledge. Statements about the Sport Head ID describe design intent and proposed implementation, not an irrevocable commercial commitment or independent verification of the running product. No user numbers are claimed in this paper.