A whitepaper for financial institutions, payment providers and digital platforms

ProofOfID

PROOFOFID.IO

Trust Infrastructure for Payments, Open Banking and Digital Transactions

© 2026 ProofOfID, Inc. All rights reserved.

Table of Contents

Trust Infrastructure for Payments, Open Banking and Digital Transactions 1

Executive summary 2

The trust gap 3

Open data, digital infrastructure and regulation 3

Open data and open finance 3
Digital public infrastructure 4
PSD2 and the path to PSD3 4
eIDAS 2.0 and European digital identity 5

From KYC to trust infrastructure 5

How it works: authorizing a payment 6

Where ProofOfID creates value 6

Platform capabilities 7

Traditional KYC compared with trust infrastructure 8

Security, privacy and compliance 8

Deployment and partnership models 9

About ProofOfID 10

Let's build trust into every digital interaction 10

Sources ..... Error! Bookmark not defined.

Legal notice 10

Executive summary

Identity verification answers one question, once: is this person who they claim to be? Payments, open banking and AI-driven transactions now ask a harder question every time money or data moves: is this party authorized, right now, to do this specific thing?

ProofOfID is trust infrastructure built to answer both. Our patent-backed platform lets institutions establish, verify, authorize and continuously maintain trusted relationships between people, organizations, AI agents and regulated services. Identity is verified once, reused with consent, and checked again at the moment of every transaction that matters.

For financial institutions, payment providers and digital platforms, this means:

- **Less fraud** at onboarding, at login and at the point of payment, not only at account opening.
- **Faster customer journeys**, because a verified identity is reused instead of re-collected.

© 2026 ProofOfID, Inc. All rights reserved.

- **Consent that regulators can audit**, specific to a purpose, limited in time or revocable by the user.
- **No central store of personal data** for attackers to target, thanks to a decentralized architecture.
- **One trust layer across channels and sectors**, from mobile banking to in-branch, telecom, healthcare and government.

Identity verification is where trust starts, not where it ends.

The trust gap

Fraud has moved from the front door to the moment money moves. A customer can pass every onboarding check and still be manipulated, impersonated or replaced by a machine later in the relationship. Four shifts are widening that gap.

- **Scams target the payment, not the account.** Global scam losses reached an estimated $62 billion in 2025, growing more than twice as fast as traditional bank fraud (Nasdaq Verafin, 2026). In the UK alone, authorized push payment fraud rose 19% to £576.4 million, and two-thirds of cases began online (UK Finance, 2026). In these cases the customer is real; it is the authorization that has been compromised.
- **AI makes identity cheap to fake.** Deepfakes and synthetic identities now defeat checks that once worked. In the United States, new account fraud was the only category whose losses grew in 2025, reaching $7 billion across 5.4 million victims (Javelin Strategy & Research, via AI2Work).
- **AI agents now initiate transactions.** In June 2026, Visa partnered with OpenAI to support agent-led payments, and Mastercard launched a service for agent-to-agent transactions (Digital Commerce 360). Every party in that chain needs to know who approved a payment, what the agent was allowed to do, and who is accountable.
- **Open banking runs on consent.** Data sharing between institutions depends on consent that is explicit, purpose-specific, time-bound and provable to a regulator. Most identity systems were never designed to record it.

Underneath all four sits a structural weakness: centralized stores of personal data. Every new database of verified identities becomes a target, and every breach feeds the next wave of synthetic and account-takeover fraud.

The gap, then, is not between knowing and not knowing who a customer is. It is between knowing who they are and knowing whether this action, by this party, at this moment, is authorized.

Open data, digital infrastructure and regulation

Open banking is growing into open data, and digital identity is becoming national infrastructure. Both depend on the same two things: knowing who is asking, and being able to prove they consented.

Open data and open finance

Open banking began with customers directing their bank to share account data with a licensed third party. Many markets are now extending that model to savings, investments, insurance, pensions and data held outside finance.

© 2026 ProofOfID, Inc. All rights reserved.

Every new data-sharing connection raises the same questions: is each party who it claims to be, what exactly did the customer agree to share, for how long, and can they withdraw it? ProofOfID answers them as one trust layer:

- **Verified parties.** People, businesses and AI agents are verified before any data moves.
- **Consent per purpose.** Each consent names what is shared, with whom and for what, and carries an expiry date.
- **Revocation that sticks.** When a customer gives revoke or reject consent, access will not be granted.
- **Evidence for regulators.** Every grant, use and withdrawal of consent is recorded in an audit trail.
- **No new honeypot.** Because data is decentralized, opening up data sharing does not create a new central store to attack.

Digital public infrastructure

Governments increasingly treat digital identity, payments and data exchange as shared national infrastructure. Infrastructure on that scale needs a trust layer that is interoperable, private by design, resilient and controlled by citizens rather than by any single company.

ProofOfID is built for that role:

- **One identity across sectors.** A verified identity can be reused in banking, telecom, healthcare, education and government services.
- **Data sovereignty.** The platform can be deployed in-country, so identity data stays under national jurisdiction.
- **Citizen control.** People decide which service sees which attributes, and for how long.
- **Public-private delivery.** Governments and institutions can deploy directly or through local partners who sell, implement and support the platform.

PSD2 and the path to PSD3

PSD2 made strong customer authentication (SCA) mandatory across the European Union and opened bank data to licensed third parties. Its successors, PSD3 and the Payment Services Regulation (PSR), reached final compromise texts in April 2026, with most obligations expected to apply during 2028 (PwC).

The new rules raise the bar on exactly the problem ProofOfID solves. Under PSD3, a successful authentication will no longer prove on its own that a payment was legitimately authorized, and the burden of proof will sit with the payment provider. Providers will also need SCA for high-risk actions such as adding a new payee, and will carry more liability for impersonation fraud.

PSD2 / PSD3 requirement	How ProofOfID supports payment providers
Strong customer authentication	Multi-factor authentication combining the customer's verified identity, their device and biometrics
Proof that a payment was authorized	A consent and authorization record for each transaction, not only a login event

© 2026 ProofOfID, Inc. All rights reserved.

PSD2 / PSD3 requirement	How ProofOfID supports payment providers
SCA for high-risk actions	Step-up authorization when adding payees, changing limits or making unusual payments
Impersonation and push payment fraud	Confirms the real customer approved this specific payment before funds move
Secure open banking access	Verified third parties and consent that is purpose-specific, time-limited or revocable

eIDAS 2.0 and European digital identity

eIDAS 2.0 sets out Europe's vision for digital identity: identity that citizens control, share selectively and reuse across public and private services. Member states must make European Digital Identity Wallets available by December 2026, and banks must accept them for strong customer authentication by December 2027 (Worldline).

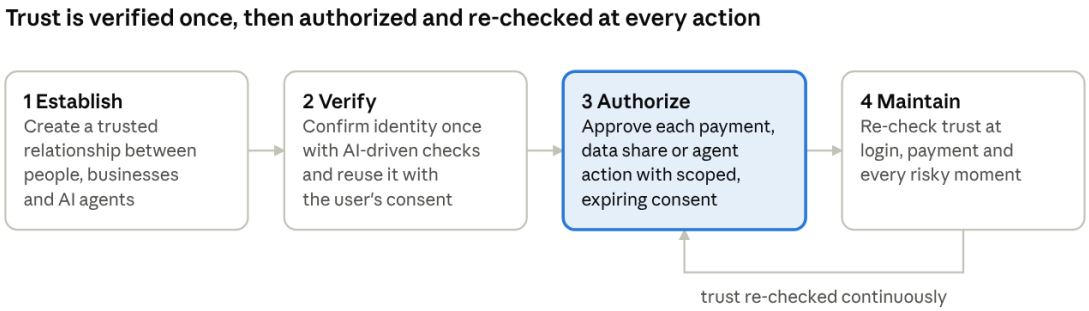
ProofOfID is built on the same principles and is designed to complement wallet-based identity, adding consent and transaction-level authorization to the journeys where wallets are used.

eIDAS 2.0 principle	ProofOfID
Citizens control their identity	Users decide who sees their identity, for what purpose and for how long
Share only what is needed	Purpose-specific sharing instead of handing over full identity records
Verify once, reuse everywhere	A verified identity reused across institutions and sectors
Trust between relying parties	Verified parties and auditable consent on every exchange
Privacy by design	Decentralized data, with no central store of personal information

From KYC to trust infrastructure

ProofOfID treats trust as a lifecycle, not a single check. Verification happens once; authorization happens every time it matters.

© 2026 ProofOfID, Inc. All rights reserved.

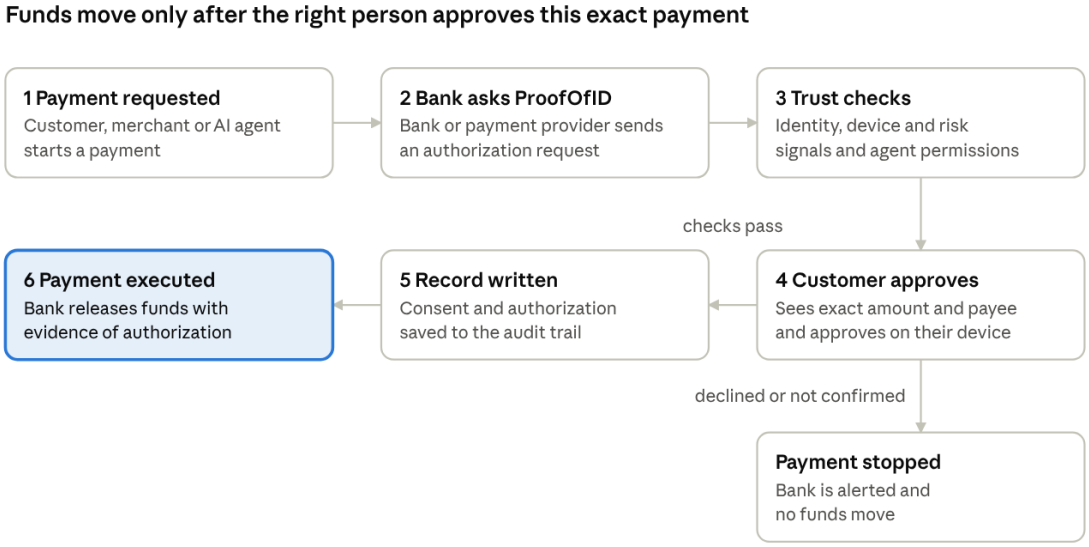


ProofOfID trust lifecycle

KYC covers only the first two stages. ProofOfID adds the last two, where most payment and account-takeover fraud now happens, and loops back to authorization for every new transaction.

How it works: authorizing a payment

Every payment that matters is authorized at the moment it happens, not assumed from an earlier login. The same flow applies to data-sharing requests and actions taken by AI agents.



Payment authorization flow

The bank keeps control of the payment decision. ProofOfID supplies the evidence: who approved, what they approved, on which device and when, so the institution can show that a transaction was genuinely authorized if it is ever disputed.

Where ProofOfID creates value

The same trust layer serves every point where money, data or access changes hands.

© 2026 ProofOfID, Inc. All rights reserved.

Use case	The problem today	What ProofOfID does	Outcome
Payments	A verified customer is tricked into approving a transfer, or an account is taken over after onboarding	Confirms the right person, on the right device, approved this specific payment before funds move	Fewer authorized push payment and account-takeover losses
Open banking	Consent for data sharing is hard to capture, prove and revoke across institutions where applicable	Records consent per purpose, with an expiry, that the user can request revoke at any time	Auditable data sharing that meets regulatory expectations
High-value transactions	Loans, property, vehicle sales and wealth transfers rely on documents and manual checks	Reuses a verified identity and adds step-up authorization for sensitive actions	Faster closing with lower impersonation risk
AI agent authorization	Agents act for people and businesses with no standard way to prove who delegated what	Binds each agent to a verified principal, with scoped, time-limited permissions	Agent-initiated transactions institutions can trust and audit
Customer onboarding	Customers repeat the same checks at every institution, and many abandon the process	Lets customers share a verified identity, with consent, instead of starting again	Faster onboarding and lower verification costs
Cross-sector services	Telecom, healthcare and government each verify the same person separately	One trust layer works across sectors and channels: online, mobile and in person	Consistent trust and a simpler customer experience

Platform capabilities

ProofOfID is a patent-backed, fully managed SaaS platform. Its capabilities work together as one trust layer rather than as separate point products.

- **Decentralized architecture.** Personal and identity data is not held in a central database. There is no single honeypot to breach, which lowers both fraud exposure and the compliance burden of holding customer data.
- **Trust to Authorize.** Every request to share identity or approve an action carries explicit user consent that is specific to a purpose, limited in time or revocable. Each decision leaves a real-time audit trail.
- **Reusable digital identity.** Customers verify once and share their verified identity with other services through QR codes or a one-time number, on their own terms.
- **AI and ML-driven validation.** Document checks, biometric matching and liveness detection are combined with risk signals to stop deepfakes, synthetic identities and impersonation.

© 2026 ProofOfID, Inc. All rights reserved.

- **Continuous assurance.** Trust is re-checked at login, at payment and at any high-risk action, so it reflects the present rather than the day of onboarding.
- **Agent delegation.** People and organizations can authorize AI agents to act for them within defined limits, and revoke that authority at any time.
- **Encrypted end to end.** Data is encrypted in transit and at rest, using modern authentication methods in place of passwords.
- **Omni-channel by design.** The same verified identity works online, in mobile apps and in person, through APIs and SDKs that fit existing systems.

Traditional KYC compared with trust infrastructure

Traditional KYC checks identity once. Trust infrastructure keeps checking whether each action is authorized.

	Traditional KYC	ProofOfID trust infrastructure
Scope	Identity at onboarding	Identity, consent and authorization across the whole relationship
Verification time	Hours to days, often with manual review	Under 5 seconds
Reuse	A new check at every institution	Verify once, reuse with consent
Payment protection	None after the account is opened	Authorization confirmed at the moment of payment
Consent	Captured once, hard to prove or revoke	Purpose-specific, time-limited, revocable and audited
AI agents	Not supported	Delegated, scoped and revocable agent authority
Data storage	Central databases of personal data	Decentralized, with no central honeypot
Operating cost	Repeated checks and manual reviews	Up to 30% lower KYC operational costs

Security, privacy and compliance

ProofOfID is built for regulated industries in every market where it operates. Privacy and auditability are part of the architecture, not features added afterwards.

Standard or requirement	How ProofOfID supports it
SOC 2	Security controls aligned with SOC 2

© 2026 ProofOfID, Inc. All rights reserved.

Standard or requirement	How ProofOfID supports it
GDPR (European Union)	Data minimization, purpose-specific consent and the user's right to revoke
PSD2 and PSD3/PSR (European Union)	Supports strong customer authentication and transaction-level authorization for payment providers, and is designed for the stricter fraud and authentication rules coming under PSD3 and the PSR
eIDAS 2.0 (European Union)	Built on the same principles of user control, selective sharing and reusable identity, and designed to complement the European Digital Identity Wallet
PIPEDA (Canada)	Aligned with Canada's federal privacy legislation
KYC	Automated identity verification built into every workflow
AML	Allows features to compliment broader AML and PCMLTFA guidelines and policies.
Open banking and data-sharing rules	Consent records that are explicit, time-bound and auditable

For institutions operating across borders, ProofOfID can be deployed in-region to meet local data residency requirements, and its consent and audit settings can be configured for each jurisdiction.

Deployment and partnership models

Institutions can adopt ProofOfID directly or through the technology providers they already use.

Model	Best for	What it includes
Dedicated managed SaaS	Banks, large financial institutions, governments	A dedicated environment, deployable in-region, fully operated by ProofOfID
Multi-tenant SaaS	Credit unions, fintechs, small and mid-sized businesses	Fast setup on shared infrastructure with tiered plans
Embedded or white-label	Core banking, digital banking and payment platforms	ProofOfID inside the partner's product, under the partner's brand
Reseller and regional partners	New markets and sectors	Local partners sell, implement and support, with ProofOfID behind the platform

All models connect through APIs and SDKs, so institutions can start with one use case, such as onboarding or payment authorization, and extend from there.

© 2026 ProofOfID, Inc. All rights reserved.

About ProofOfID

ProofOfID, Inc. is a Canadian technology company with a global presence, building trust infrastructure for the AI economy. Founded in December 2022 by François Roukoz, a seasoned fintech and banking entrepreneur, the company is led by the founder and an experienced leadership team with diverse technical and business expertise across fintech and technology.

- **Patent-backed** proprietary platform
- **Member** of the Digital ID and Authentication Council of Canada (DIACC) since 2024
- **Member** of the Open Banking Expo (OBExpo) Canada, UK & EU since 2024
- **Finalist**, Open Banking Expo Awards 2025: Best Anti-Fraud Solution
- **Finalist**, Open Banking Expo Awards 2026: Best Open Banking Infrastructure - Platform Provider

Mission: To establish trust in every digital interaction by delivering a secure, customer-focused identity solution that protects privacy, reduces fraud, and meets regulatory requirements.

Let's build trust into every digital interaction

The institutions that win the next decade of payments and open banking will be the ones customers, regulators and partners can trust at every transaction, including those made by AI agents.

See ProofOfID in action. Request a demo at www.proofofid.io/contact.

Legal notice

This whitepaper is provided for general information only. It does not constitute legal, regulatory, financial or compliance advice, and should not be relied on as such. References to laws and regulations, including PSD2, PSD3, the Payment Services Regulation, eIDAS 2.0, GDPR and PIPEDA, describe how ProofOfID is designed to support institutions; they are not a statement that any institution's use of ProofOfID satisfies all its legal obligations. Responsibility for regulatory compliance remains with each institution, which should seek its own legal advice.

Product capabilities, performance figures and regulatory timelines are stated as of the date of publication and may change. Third-party figures are drawn from the sources listed and have not been independently verified by ProofOfID.

© 2026 ProofOfID, Inc. All rights reserved.