

Is razorpay.com legit? TrustSniffer's high-trust assessment: 90/100

razorpay.com

Verdict

90

OUT OF 100

HIGH TRUST

razorpay.com appears legitimate.

Our checks found nothing pointing to fraud. Ordinary care still applies when you pay or sign in.

Not Scam

Low Risk

Assessed 2026-08-11 by automated analysis. Classification confidence 75%.

What this site appears to be

Corporate landing and product site for Razorpay: describes payments, payouts, business banking, payroll, developer APIs, and related fintech products. Contains marketing copy, developer docs snippets, and trust signals such as partner banks and registered office address.

Evidence status and limitations

- Evidence completeness: UNKNOWN
- The real-world operator identity was not independently verified.
 - Module-level completeness metadata is unavailable for this legacy report.

At a glance

The checks that decide most of this verdict.

Malware engines	None flagged it VirusTotal	CLEAR
Google Safe Browsing	Not listed Google	CLEAR
Abuse reports on the host	0 reports AbuseIPDB; shared hosting inflates this count	NOTED
Domain age	16 years old Registered history	CLEAR
Web archive	Archived since 2011 2152 snapshots	CLEAR
Certificate	Encrypted connection Issued by Amazon RSA 2048 M01	NOTED

The page as captured

No screenshot is retained for this report.

Key findings

- Automated classification: Not Scam.
- Domain age: more than 10 years (registration continuity).
- Public web-archive history exists since 2011.
- No flags from the reputation services TrustSniffer consulted at assessment time.

Full analysis

Overview

Razorpay.com is a corporate fintech product website presenting payment processing, payouts, business banking, payroll automation, developer APIs, and related services for businesses. Its apparent business model is to support merchant and enterprise financial operations through transaction fees, banking and service fees, credit-related products, payroll services, and integrations.

Scam/Impersonation Risk

No contradictions were observed: the available evidence contains no phishing, impersonation, confirmed blacklist, or malicious-reputation indicators. The homepage presents a coherent corporate payments business rather than a deceptive investment or consumer fraud proposition, and observed browsing behavior showed no login form, hidden sensitive form, wallet-drainer activity, clipboard hijacking, cloaking, or suspicious inline scripts. The site's long, continuous presence and clean external reputation materially support an apparently legitimate, established-site assessment, although they do not independently prove the real-world operator's identity.

EVIDENCE

- The homepage describes payment acceptance, payouts, business banking, payroll automation, in-store payments, and developer integrations, with no page-level red flags recorded.
- Browser interaction testing completed 2 runs successfully; 0 hidden forms, 0 wallet-connect runs, 0 wallet-drainer runs, 0 clipboard-write events, and 0 suspicious inline scripts were observed.
- The domain was registered on 2013-08-23 and has a recorded WHOIS age of 12.97 years; registrar: Gandi SAS.
- The web archive records 2,152 snapshots spanning 2011-02-02 through 2026-07-19, covering 16 years with a maximum gap of 1 year.

Regulatory Verification Notes

The site appears to operate as an established payments and financial-technology business, and its pages reportedly include a registered office address and references to partner banks. However, the available evidence does not independently verify the legal operator or a regulatory authorization, and the on-page disclosure state is unclear. This is a regulatory and transparency verification point rather than evidence of a scam. The domain uses privacy-protected ownership records, which is an administrative limitation; it does not create an identity contradiction. External reputation checks were clean, and no broker-dataset match was identified, but these signals are contextual rather than legal or licensing determinations.

EVIDENCE

- The homepage and related corporate content describe a professional payments/fintech business and reference partner banks and a registered office address.
- The site's transport encryption uses a DV certificate issued by Amazon RSA 2048 M01, valid through 2026-11-04.
- The site is served from AS16509, Amazon.com, Inc. (AMAZON-02), US.
- Page-authority assessment places the site in a high authority band; external checks recorded 0 malicious and 0 suspicious detections, with no blacklist hit.

What to Verify Next

Before credential or payment interactions, an enterprise or consumer counterparty should independently confirm the applicable Razorpay legal entity and any relevant payment, lending, banking, or payroll authorization with the competent jurisdictional registry. The counterparty should also review the applicable terms, privacy, refund or merchant-service provisions, and payment-protection arrangements, and confirm official support channels through an independently sourced route rather than relying solely on page links.

EVIDENCE

- The homepage contains sign-up and login navigation but no sensitive form was rendered during the observed capture.
- The site describes multiple financial services whose regulatory treatment may differ by jurisdiction and product.
- The available evidence identifies Gandi SAS as registrar and Amazon RSA 2048 M01 as certificate issuer, but these technical facts do not independently establish the operating legal entity.

Summary Verdict

Available evidence is consistent with an established, apparently legitimate website and supports a high-trust, low-risk posture with no observed scam or impersonation contradictions. The assessment supports normal website interaction in principle, while the real-world operator identity remains independently unverified.

Infrastructure Integrity

The website is protected by Amazon CloudFront CDN/WAF infrastructure and is hosted through Amazon.com, Inc. This mainstream protective architecture and the presence of CDN edge infrastructure mitigate direct exposure and improve delivery resilience, but infrastructure protection is not, by itself, proof of legitimacy.

Closing Assessment

Ordinary use may proceed subject to the proportionate checks above, with independent confirmation of merchant identity, applicable authorization, return or service terms, and payment protections before credentials or funds are committed.

Written analysis generated 2026-08-11 by the TrustSniffer Analysis Engine from the evidence in this report.

What the analysis found

No rule findings contributed to this verdict.

Identity verification

Status	UNVERIFIED
Identity score	30/100
Identity verification confidence	25%

- No on-site identity signals detected

Identity verification measures whether the site can be independently connected to a real-world brand or person. It is separate from the classification confidence.

What TrustSniffer observed

First-party facts recorded during the assessment of razorpay.com.

- The request stayed on razorpay.com. It was not redirected to another domain. CLEAR
- Registration is published under Gandi SAS. CLEAR
- DNS for this domain is served by awsdns-47.org, across 4 name servers. NOTED
- The registration is paid up to 2027-08-23. NOTED
- The earliest public archive of this site is from 2011-02-02. CLEAR
- It is hosted on AMAZON-02, from a server in US. NOTED

Domain intelligence

Registrar	Gandi SAS
Hosting	AMAZON-02 - Amazon.com, Inc., US
Country	US
Server IP	52.85.154.117
Name servers	NS-1400.AWSDNS-47.ORG, NS-1939.AWSDNS-50.CO.UK, NS-723.AWSDNS-26.NET, NS-74.AWSDNS-09.COM
SSL issuer	Amazon RSA 2048 M01
SSL expiry	2026-11-04
Domain age	15.52 years (continuous registration)
Domain expiry	2027-08-23
Archive first seen	2011-02-02
Archive snapshots	2152
Reputation	VirusTotal: 0 flagged AbuseIPDB: 0 reports Google Safe Browsing: 0 matches

About this assessment

A trust score summarises the evidence TrustSniffer could collect about razorpay.com at assessment time. It is a starting point for your own judgement, not a guarantee: a high score means the signals were consistent with a

legitimately operated site, a low or critical score means several risk patterns were present.

TrustSniffer assesses a website from the evidence it can collect at a point in time: domain registration and age, hosting and certificate, the content the site served, and third-party reputation feeds. A score is a summary of that evidence, not a guarantee and not a legal finding. There is no human rating and no user review in it. A site can change after it is assessed.

This report online: <https://trustsniffer.com/report/razorpay.com> · assessed 2026-08-11