✓ Proofline

FREE TEMPLATE

Fintech API testing checklist

Idempotency, money handling, authorization, SCA, webhooks, limits and reconciliation – the checks we run on payment APIs.

> For payment, banking and card APIs. Maps to the OWASP API Security Top 10 (2023) and common PSD2 requirements. Use a dedicated test tenant and the provider's sandbox – never real customer data.

1. Money handling

	CHECK	PRIO	OWNER / NOTE
☐	Amounts use integer minor units or decimal types – never floating point; test 0.1 + 0.2 style cases.	HIGH	
☐	Currency exponent respected (JPY 0, EUR 2, BHD 3 decimals); unsupported currencies rejected.	HIGH	
☐	Boundaries: 0, negative, minimum, maximum, max+1, very large numbers, more decimals than allowed.	HIGH	
☐	Rounding rules documented and tested for FX, fees and splits (sum of parts equals total).	MED	
☐	Limits (per transaction, daily, monthly) enforced server-side, including concurrent requests.	MED	

2. Idempotency & concurrency

	CHECK	PRIO	OWNER / NOTE
☐	POST payment/transfer supports an Idempotency-Key; the same key + same body returns the original result.	HIGH	
☐	Same key + different body is rejected (e.g. 422), not silently processed.	HIGH	
☐	Parallel duplicate requests (race) create exactly one transaction; balance never goes below allowed minimum.	HIGH	

☐	Client timeouts and retries: the outcome is retrievable (GET by reference) without double charging.	MED	
☐	State machine transitions enforced (e.g. cannot refund a pending or already-refunded payment).	MED	

3. Authentication & authorization (OWASP API1, API2, API5)

	CHECK	PRIO	OWNER / NOTE
☐	BOLA: every object ID (account, payment, payee, card) is checked against the caller; test with a second tenant's IDs.	HIGH	
☐	Function-level authorization: customer tokens cannot call admin/back-office endpoints.	HIGH	
☐	Tokens: expiry, revocation, audience/issuer validation, alg=none and key-confusion rejected.	HIGH	
☐	OAuth2 scopes are least-privilege and enforced per endpoint.	MED	
☐	401 vs 403 vs 404 responses do not leak existence of other customers' resources.	MED	

4. Strong customer authentication (PSD2 / SCA)

	CHECK	PRIO	OWNER / NOTE
☐	SCA triggered where required (payment initiation, new payee, sensitive data); exemptions applied only per rules.	HIGH	
☐	Dynamic linking: the authentication code is bound to amount and payee; changing either invalidates it.	HIGH	
☐	OTP/challenge: limited attempts, expiry, no reuse, rate limited per user and per device.	MED	
☐	3-D Secure flows (frictionless, challenge, failure, timeout) tested with the acquirer's test cards.	MED	

5. Input validation & data exposure (API3, API8)

	CHECK	PRIO	OWNER / NOTE
☐	IBAN/BIC, sort code, card numbers validated (checksum) and never echoed in full; PAN masked, CVV never stored or returned.	HIGH	
☐	Mass assignment: clients cannot set status, balance, fee, owner or KYC fields.	HIGH	
☐	Responses contain only needed fields; no internal IDs, stack traces or other customers' data.	MED	
☐	Unicode, very long strings, injection payloads in references/descriptions handled safely end-to-end (incl. exports/CSV).	MED	

6. Webhooks & callbacks

	CHECK	PRIO	OWNER / NOTE
☐	Webhook signatures verified (HMAC + timestamp); replayed or unsigned events rejected.	HIGH	
☐	Handlers are idempotent: duplicate and out-of-order events do not double-book.	HIGH	
☐	Retries with backoff; dead-letter handling and alerting tested.	MED	
☐	Outbound callback URLs validated against SSRF (no internal addresses).	MED	

7. Reliability, limits & performance (API4)

	CHECK	PRIO	OWNER / NOTE
☐	Rate limits per client/key with 429 + Retry-After; expensive endpoints (search, exports, statements) bounded.	HIGH	
☐	Pagination with enforced maximum page size on all list endpoints.	HIGH	
☐	Load test at month-end / payday peaks; p95/p99 and error-rate thresholds defined in k6.	MED	
☐	Downstream failures (core banking, card processor, KYC provider) produce clear, retry-safe errors; circuit breakers tested.	MED	

8. Ledger, reconciliation & audit

	CHECK	PRIO	OWNER / NOTE
☐	Double-entry invariants hold after every test (debits = credits, no orphan entries).	HIGH	
☐	Daily reconciliation against PSP/bank files detects and reports mismatches.	HIGH	
☐	Audit log for sensitive actions (who, what, when) is immutable and excludes secrets.	MED	
☐	Time zones and cut-off times (end of day, bank holidays, DST) tested.	MED	
☐	API versioning and deprecation policy tested with old clients.	LOW	

© Proofline · Free template, may be used and adapted internally. Not legal advice.