SiGi Technologies

Facts as of November 1, 2026

FINTECH SECURITY CHECKLIST

20 controls to protect payment workflows

Use these questions to find the areas that need a closer look. An unticked item does not mean you are vulnerable; it means the control should be checked or documented. Where an item lists evidence, that is what to look for.

1 OF 5

Access and infrastructure

- [ ] **Production permissions match each person's and service's actual job.**
  Evidence: an access review in the last 90 days, with unused permissions removed.
- [ ] **Payment and payout infrastructure is isolated from general application workloads.**
- [ ] **Production access is time-limited, logged and reviewed.**
  Evidence: production access requests show an expiry time and a reason in the logs.
- [ ] **Compromised credentials can be revoked and rotated within minutes.**
  Evidence: a timed drill, with the result written down.

2 OF 5

Payments and sensitive operations

- [ ] **Payment, refund and payout decisions are validated on the server.**
  Evidence: changing an amount or order ID in an API request is rejected server-side.
- [ ] **The identity requesting a payout cannot bypass its authorization controls or independently execute it.**
  Evidence: an authorization test shows the requesting identity cannot bypass approval rules, modify risk limits or release funds without required checks.
- [ ] **High-risk transactions need an independent approval.**
  Evidence: a test payout above the limit, or to a new beneficiary, stops and waits for approval.
- [ ] **Payments are protected against duplicates and replays.**
  Evidence: sending the same request twice with one idempotency key produces one payment.
- [ ] **Changes to beneficiaries or approval limits are treated as sensitive events.**
  Evidence: changing a payout bank account triggers an alert and a hold on the next payout.

3 OF 5

Developers and people

- [ ] **Phishing-resistant MFA protects cloud, source control and CI/CD.**
  Evidence: admin accounts cannot sign in with SMS or app-push codes.
- [ ] **No production secrets or signing keys are stored on laptops.**
  Evidence: a secret scan of developer machines and repositories comes back clean.
- [ ] **Engineers know not to run interview tasks or unknown code on work machines.**
- [ ] **Access is removed the same day someone leaves or a contract ends.**

4 OF 5

Monitoring and testing

- [ ] **Unusual payment activity or privilege changes trigger an alert someone acts on.**
- [ ] **Key authorization rules are covered by automated negative tests.**
  Evidence: tests for self-approval, duplicate payouts and split payments run on every release.
- [ ] **Cross-tenant access is tested.**
  Evidence: requests with another tenant's IDs return "not found" or "forbidden".

5 OF 5

Incident readiness

- [ ] **Money movement can be paused without taking the product offline.**
  Evidence: a documented switch, with an owner, that has been tested in staging.
- [ ] **Recovery procedures and backups are tested regularly.**
- [ ] **Security logs are protected and detailed enough to investigate.**
- [ ] **Incident owners, escalation paths and customer communication are agreed in advance.**

Ticking a box records your own assessment. It is not proof that a control works; only testing shows that.

Want a second pair of eyes on your payment workflows?

Book a free consultation: sigitechnologies.com/book-a-consultation