Payment provider evaluation checklist

corefy

1. Business model requirements

- [ ] Define your business model and ensure the provider supports your strategic goals.
- [ ] Confirm omnichannel support for payment options relevant to your audience.
- [ ] Check if the provider's payment processing fees are suitable for your business.

2. Global coverage

- [ ] Analyse popular payment options and currencies in your target geos.
- [ ] Ensure compliance with local regulations in key markets.
- [ ] Verify localisation capabilities, including languages and currencies.

3. Integration options

- [ ] Assess the provider's integration capabilities and compatibility with your existing setup.
- [ ] Evaluate the clarity and comprehensiveness of API documentation.

4. Payment provider's health

- [ ] Check the provider's system stability and uptime records.
- [ ] Ensure it's flexible enough for rapid development and expansion.
- [ ] Confirm scalability for handling peak transaction volumes.
- [ ] Assess the provider's commitment to innovation and feature updates.

5. Payment processing

- [ ] Check capabilities in handling various authorisation and capture scenarios, including incremental authorisations, extended windows, and over-captures.
- [ ] Evaluate the speed of transaction processing and settlement.

6. Risk management

- [ ] Assess built-in fraud management tools and customisation options.
- [ ] Check the provider's approach to disputes and chargeback management.
- [ ] Evaluate the fees for processing chargebacks and refunds.
- [ ] Check if the rolling reserve conditions suit you (especially for high-risk businesses).

7. Reporting and analytics

- [ ] Confirm availability of real-time, detailed transaction reporting.
- [ ] Check for custom reporting capabilities and API access for data integration.
- [ ] Evaluate the availability of tools for data analysis and visualisation.

8. Reconciliation

- [ ] Check for transaction-level reporting accuracy and availability of efficient post-settlement reconciliation.
- [ ] Confirm the availability of manual or automated reconciliation of chargebacks and refunds.

9. Privacy and security

- [ ] Confirm PCI DSS compliance and other relevant security certifications.
- [ ] Evaluate tools for minimising PCI exposure.
- [ ] Assess data transfer and storage security in compliance with regulations like GDPR.

10. Additional services and support

- [ ] Check for the availability of decent and timely customer and technical support.
- [ ] Evaluate any additional services like subscription management, invoicing, and in-person payments.
- [ ] Confirm the availability of resources for EMV certification and hardware support.

Final step

Request and review provider references and case studies. Then schedule a demo and ask for sandbox access to test the provider's service.