Basis Theory

High-Risk Merchants

A Checklist for High-Risk Payment Processing

Overview

Card networks and PSPs set their own standards for what could place a merchant in a high-risk category of payment processing.

Merchants are classified as “high risk” based on a combination of factors, which could include:

- Higher than average chargeback rates.
- Concerns of suspicious activity.
- Financial health.
- “Bad actor” reports on the account.
- Operating in “high-risk” industries, such as gaming, gambling, dating, CBD, travel, digital health, and e-commerce.

Once designated as high-risk, merchants must meet unique standards and processing requirements to continue processing payments. Failure to do so risks account shutdown.

High-risk merchants should use this checklist to work with PSPs—and stay live with payment processing.

Understand Your Risk Level

The risk level of a business determines the direction a merchant should take for payment processing and compliance.

- □ Confirm your Merchant Category Code (MCC).
- □ Understand your risk tier.
- □ Research industry regulations, including:
  - □ PCI DSS regulations for compliance.
  - □ Additional industry-specific regulations, for instance, in gaming, CBD, and digital health.
- □ Determine which level of compliance you need.

Understanding your industry and its risks can help you select the right long-term payment partners.

Choose the Right Payment Processor

Not all payment processors are created equal. Complete your due diligence to select the appropriate processor for your business upfront.

- □ Research specialized high-risk processors that work with your MCC.
- □ Understand PSP and card network fees and chargeback policies.
- □ Document a business support plan.
    - □ Anticipate higher processing costs.
    - □ Budget for potential chargebacks and losses.
    - □ Prepare for payment reserves in case of disputes or chargebacks.
- □ Be prepared for stricter underwriting requirements that may require additional documentation upfront.

Manage Security and Compliance

Should you build and maintain a cardholder data environment (CDE) or outsource to a trusted third party?

- □ What level of ownership do you want over your CDE?
    - □ No ownership; use a built-in vault through a full-service PSP.
    - □ Outsourced ownership; use a third-party token vault.
    - □ Full ownership; build in-house.
- □ How do you want to handle PCI compliance?
    - □ Offload compliance scope and expenses.
    - □ Manage compliance and scope in-house.

> *"Our PSP said they were okay with our business but they ended up going back on their word and* ***shutting us off without any warning****. We wanted to make sure that we're always in a position where we will have a provider even if something happens."*
>
> Patrick Zhang, Tech Lead at Passes
>
> Read The Case Study →

Maintain an Excellent Customer Experience Program

Even with the best fraud reduction techniques, operating in higher-risk industries can mean a higher rate of chargebacks and disputes. Being upfront with your offerings and building a transparent checkout process can significantly reduce the number of negative remarks from customers.

- □ Ensure you’ve built a user-friendly checkout flow.
    - □ Follow our UX checkout tips.
- □ Address (both negative and positive) customer feedback and requests promptly.
- □ Iron out the details needed to go live with your PSP.
    - □ If switching from another PSP, take steps to reduce negative impacts.
    - □ Publish a privacy policy.
    - □ Publish terms and conditions.

Working with a Payment Vault for Flexibility and Compliance

Did you know you can remove your front-end applications entirely from PCI compliance scope?

A solution like Basis Theory Elements empowers merchants to:

- Build a payment flow to their specifications
- Route transactions appropriately
- Connect their preferred partners
- Maintain PCI compliance

...all without bringing systems into PCI scope.

Contact us today to start creating your secure payment flow.