Basis Theory

High-Risk Payment Processing

What High-Performance Merchants Should Know

Table of Contents

The Rules of the Game

What are the Guidelines for Designating a Business as High Risk?

While there are many guidelines in place that designate a business as high risk, there's also a bit of an art and a science behind it.

For the most part, the card networks (Visa, Mastercard) determine which companies are of higher risk. Each brand has its own set of rules that merchants must understand and follow when operating in "higher" risk businesses.

Visa Integrity Risk Program (VIRP)

Through April 30, 2023, the Visa Global Brand Protection Program (GBPP) was Visa's compliance program addressing the reputational risk and potential brand damage for acquiring merchants in high-risk verticals. Beginning on May 1, 2023, the Visa Integrity Risk Program (VIRP) replaced this program.

According to the Visa Integrity Risk Program Guide, "VIRP ensures that Acquirers, and their designated agents, maintain proper controls and oversight processes to deter illegal transactions from entering the Visa Payment System."

Three major changes distinguish VIRP from GBPP:

1. High-risk merchants now fall under three tier levels
2. Updated, modernized language for high-risk merchants
3. Categories for Visa control assessments

The Mastercard Business Risk Assessment and Mitigation (BRAM)

BRAM differs from VIRP in that it focuses more on finding and addressing non-compliance with the Mastercard rules. When a merchant is found to be out of compliance with the standards, acquirers are required to add the merchant to the Mastercard Alert to Control High Risk Merchants (MATCH) database.

MATCH is essentially an informational exchange between acquiring banks that allows merchant acquirers to review enhanced information about a merchant's risk prior to entering into an agreement with them.

A merchant is required to be added to MATCH within 5 days of any acquirer deciding to terminate a relationship with a merchant.

Merchant acquirers are required to submit a MATCH inquiry prior to onboarding a merchant.

Should the merchant be found on the MATCH list, the acquirer must then decide if it would like to do business with the merchant but is not discouraged from doing so.

Merchants can only be removed from the MATCH database for two reasons: the merchant was added in error, or the merchant was added for reason code 12 (PCI non-compliance) and has since become compliant. After 5 years, regardless of reason a merchant is automatically removed from the database and the MATCH program.

Which Elements are Reviewed When Determining Risk Status?

When regulatory bodies review data to determine if a business represents higher risk, several factors influence the decision.

Underwriting and MCCs

A Merchant Category Code (MCC) is a four-digit number used to categorize merchants based on their business activities and products or services being sold.

Subject to credit card association guidelines, MCCs are assigned to each merchant account by the acquiring bank when the merchant account is established. A single merchant may have multiple MCCs assigned that vary depending on the different products, services, or departments the company sells. Likewise, some companies may have their own dedicated MCC, like airlines, rental cars, and hotels.

The credit card associations have also established rules and regulations defining the use of particular MCC categories for risk monitoring purposes. In some instances, merchants are required to pre-register their business if it operates in specific high-risk MCC categories.

Some of the higher-risk categories include:

- Gambling
- Adult Content
- Pharmacies
- And more

Learn more about MCCs here.

Risk Types

Merchant acquirers and PSPs use a combination of automated tools and manual reviews to assess various risk types that impact merchants.

PSPs use a combination of automated tools and manual reviews to assess these risks. They may also request additional documentation or conduct on-site visits to verify information and assess the merchant's operations. By conducting thorough risk assessments, PSPs can protect themselves and their customers from financial losses, legal liabilities, and reputational damage.

Merchant acquirers and PSPs will assess risk a bit differently by bucketing the risk into types, including:

- **Content / Business Risks** - PSPs assess the nature of the merchant's products or services to identify potential legal, regulatory, or ethical concerns. They review the merchant's website, marketing materials, and customer reviews to ensure compliance with industry standards and to identify any potential red flags, such as misleading claims, false advertising, or inappropriate content.
- **Financial Risks** - PSPs evaluate the merchant's financial stability and creditworthiness to assess their ability to fulfill financial obligations and manage chargebacks. They review the merchant's financial statements, credit history, and business model to determine their financial strength and risk of insolvency.
- **Reputational Risks** - PSPs assess the merchant's reputation and public perception to identify any potential negative associations that could damage the PSP's reputation. They analyze online reviews, social media sentiment, and industry news to identify any negative publicity, customer complaints, or regulatory actions against the merchant.

- **Money Laundering Risks** - PSPs implement anti-money laundering (AML) procedures to prevent criminals from using their platform to launder illicit funds. They verify the merchant's identity, beneficial ownership, and business activities to ensure compliance with AML regulations. They also monitor transaction patterns for suspicious activity, such as large cash transactions, unusual transaction volumes, or transactions from high-risk jurisdictions.
- **Transaction Laundering Risks** - PSPs assess the merchant's risk of transaction laundering, where criminals use legitimate merchant accounts to process payments for illegal activities. They review the merchant's website, products, and transaction history to identify any discrepancies or inconsistencies that could indicate transaction laundering. They also monitor for unusual transaction patterns, such as spikes in transaction volume or transactions from unrelated industries.

Business and Sales Model

The merchants' business and sales model can also designate whether a business operates as high or low risk. When operating in a model that is known to have higher risks for chargebacks, customer disputes, or fraud, PSPs and acquiring banks may be apprehensive to do business.

Risk factors found in business models that may elevate a company's risk include recurring billing, subscriptions, and free trials.

A breakdown of the risk factors into which issues may arise include:

Issue	Risk Factors	Details
Increased Chargebacks	Recurring billing Subscriptions	Because these often involve automatic charges to customers' cards, they can lead to unintentional or unauthorized charges.
Customer Disputes	Subscriptions Free Trials	If customers feel misled or did not receive expected value, they may dispute the charge. If they were not informed about automatic renewals, they may dispute.
Fraud Potential	Recurring Billing Free Trials	Malicious actors may sign up for services using stolen credit card information or attempt to abuse the free trial system.

Fraud Flags

A final, more nebulous element is that of “fraud flags”. While this is not an official definition, this is somewhat of a catch-all for when a few factors - even some that may not inherently cause a business to be high-risk - combine to designate a business as higher risk.

This could be a mixture of fraud elements and the business vertical.

For example, let’s take the case of a cross-border tobacco organization that opened a Merchant Account under an MCC of 5993. This MCC falls into Tier 3 of the VIRP where there is a higher risk of non-compliance without appropriate controls, but doesn’t inevitably make processing more expensive or more challenging.

However, after a year, this business begins to experience an increasing number of chargebacks, sitting at 0.85%. This is still below the Visa and Mastercard thresholds for risk, but is quite high.

Then, the company experiences a small data breach due to a vulnerability that was never addressed. This leads to a PCI compliance audit, a Visa audit, and puts the organization on the MATCH list. At this point, the company would now be considered high-risk and will likely need to work with a payment processor that specializes in high-risk business to continue operating.

How Are Merchants Shut Down?

Why Would a High-Risk Company Be Shut Down?

We covered this a bit in the first post of the series discussing the rules of the high-risk payment processing game. Fundamentally, the reasons that a company would be designated as high risk in the first place are likely to be the cause of a company being prevented from transacting.

In short, some of these reasons could be:

- **High chargeback rates** - if a merchant exceeds the chargeback thresholds set by the card networks (0.65% for Visa and 1% for Mastercard), they may incur fines. If they are

considered excessive amounts (1.5% or higher), then the merchant account could be terminated.

- **Operating in a risky business** - just by the pure nature of being in a "riskier" business, a merchant could be shut down by a PSP even with no prior issues. This could be due to the PSP hedging against what could be a potential issue eventually, or due to that PSP no longer wanting to operate in that space.

However, the rules aren't hard and fast, and the process is tricky: everyone is managing their own level of risk.

What is the Process of a High-Risk Merchant Being Shut Down?

To put it simply, the card networks will notify a merchant acquirer if any of their merchants experience chargebacks above the network's threshold. It is then up to the acquirer to decide how to handle the next steps with the merchant.

In rare cases, the acquirer (in many cases, an all-in-one PSP), can choose to prevent the merchant from transacting at any point without warning. The PSP can shut down the account and require the merchant to leave the platform. They may also retain funds that are owed to the merchant for a period of time in anticipation of future refunds or chargebacks, further hurting the merchant's cashflow.

In more common situations, however, acquirers will give the merchant a warning period in alignment with the warning period defined by the card networks.

In yet other cases, PSPs may do a mix of following card network guidance and their own internal system rules to determine next steps and potential shutdown procedures.

Visa Dispute Monitoring Program (VDMP)

At the end of each month, Visa calculates the dispute rates for that month for each merchant.

If a merchant exceeds 75 disputes or a dispute ratio (disputes-to-transactions) of 0.65%, the merchant will be on Early Warning. This does not mean the merchant is officially on the VDMP but that it needs to be cautious of chargebacks in order to avoid inclusion on the list.

However, If a merchant meets or exceeds 100 disputes with a 0.9% dispute ratio, the merchant will be placed in the VDMP.

Visa Program Threshold	Disputes	Ratio
Early Warning	75	0.65%
Standard	100	0.9%
Excessive/High-Risk	1,000	1.8%

Further, a merchant will move from the VDMP standard program to the VDMP high-risk program if the merchant hits the excessive risk threshold of 1,000 disputes and a dispute ratio of 1.8% in a month.

Any merchant that is moved to the VDMP high-risk program because it exceeded the excessive dispute threshold will continue to be monitored under the VDMP high-risk program until the Merchant exits the VDMP (that is, gets below the threshold of inclusion at 100 disputes and a 0.9% dispute ratio) regardless of whether the merchant gets below the excessive threshold. It is also highly likely that PSP partners will levy additional fees, and ramp up the per-unit cost for each chargeback.

Any merchant that changes acquirers or country locations will also bring its VDMP program inclusion status (or an equivalent status) until deemed ready to leave the program.

A merchant will exit the VDMP if it can remain below the program thresholds for three consecutive months.

VDMP Standard Program timeline

Once placed on the VDMP, Visa will continue to monitor the merchant's disputes and ratio to determine next action. This monitoring includes all disputes listed in Visa's Dispute Management Guide.

Should a merchant fall into the standard program for an extended period of months, acquirers and merchants will be required to provide ongoing documentation of remediation efforts, and both parties may begin to be fined by Visa. After 12 months of not getting below the threshold, the merchant may be no longer allowed to transact with Visa.

Program Status	Visa's Stated Actions
Month 1: Notification	Within 10 calendar days of exceeding the thresholds, the merchant will be notified by the acquirer. The acquirer must review activity and research the cause of the excessive disputes.
Months 2-4: Workout Period	From month 2 onwards: The acquirer has to implement a Dispute remediation plan for the merchant and provide required documentation to Visa. From month 3 onwards: acquirer provides Visa written updates of the Dispute remediation plan.
Months 5-11	From month 5 onwards: the acquirer may face fees (and will almost certainly pass these to the merchant). Month 8: Acquirer must send Visa written confirmation that the merchant has been notified that it may lose Visa acceptance privileges if it fails to reduce its disputes below the program thresholds by month 12. Month 10: review fees are applicable (and may pass to the merchant).
Month 12	Non-compliance assessments and fees may occur and the merchant may be eligible for disqualification.

VDMP High-Risk Program timeline

Should a merchant fall into the high-risk program for an extended period of months, acquirers and merchants will be required to provide ongoing documentation of remediation efforts, and fines will begin almost immediately. After 12 months of not getting below the threshold, the merchant may be no longer allowed to transact with Visa.

Program Status	Visa's Stated Actions
Month 1: Enforcement Period	Within 10 calendar days of exceeding the thresholds, the merchant will be notified by the acquirer and non-compliance assessments and fees may occur. The acquirer will have to review activity and research the cause of the excessive disputes. A remediation plan should be created.

Months 2-5: Enforcement Period	Non-compliance assessments and fees will occur. Acquirers must work with merchants to ensure the remediation plan is effectively reducing disputes and provide monthly written documentation to Visa signaling this.
Months 6-11: Enforcement Period	Non-compliance assessments and fees will occur. Acquirers must work with merchants to ensure the remediation plan is effectively reducing disputes and provide monthly written documentation to Visa signaling this. Month 6: Acquirer must provide Visa with the documentation sent to merchants. Month 7: Review fees are applicable.
Month 12: Enforcement Period	Non-compliance assessments, review fees, and other fees will occur. Merchant is eligible for disqualification. Acquirers must work with merchants to ensure the remediation plan is effectively reducing disputes and provide monthly written documentation to Visa signaling this.

Mastercard Excessive Chargeback Program (ECP)

Similar to the VDMP, Mastercard has a program for when merchants pass excessive chargebacks through the Mastercard card network.

Calculated for the preceding month, a merchant is included in the ECP if they have two or more months with the following chargeback levels (does not need to be consecutive months):

Mastercard Program Level	Disputes	Ratio
Excessive Chargeback Merchant (ECM)	100	1.5% (150bp)
High Excessive Chargeback Merchant (HECM)	300	3% (300bp)

Beginning at two months, non-performance assessments will be necessary for the acquirer to complete on behalf of the merchant.

The merchant cannot be removed from the ECP until falling below the ECM threshold for three consecutive months.

What Does a Shutdown Look Like?

There are technically two types of shutdowns: shutdown by the card network and shutdown by the acquirer.

If a merchant goes through the 12 months of active communication between the merchant, acquirer, and the card networks as part of the VDMP, they will likely not be surprised to receive a notice of shutdown from both Visa and their acquirer. These merchants would likely be unable to use that PSP any further, and may also no longer be able to transact via the card network.

In other cases, the acquirer shutdown may be due to internal review of the merchant's accounts only, and not due to a Visa shutdown. In this case, the merchant would need to find a new acquirer but would still be able to transact via the card networks.

Shutdown Communication

For most all-in-one PSPs, the communication of a shutdown comes over email.

For Stripe, this shutdown notice frequently includes the following information:

- Notice of account shutdown, effective immediately
- 100% of funds being held to cover incoming transactions for the next 90 days
- 14 days to switch to a new provider before being unable to process any future transactions

After a shutdown due to excessive disputes, acquirers are required to notify the card networks - Visa will need notice of account closure and Mastercard will need the acquirer to add the merchant to the MATCH program.

Staying Operational with One PSP

How to Stay Compliant and Operational with One PSP

There are various reasons why a merchant may want to partner with a single payment service provider to process payments. Whether it is timing, resource constraints, or desire to keep data in a single system, high-risk merchants of all sizes can remain operational and reduce risks while leveraging a single PSP if they choose the right partners.

Find a Good Partner in Your Payment Service Provider

The first - and, arguably most important - partnership a high-risk merchant can make is the one with the payment service provider that will process all their payments.

Broadly speaking, merchants have two types of PSPs they may choose from: an all-in-one PSP or a specialized PSP. Each route comes with its own benefits and downsides.

All-in-one PSPs like Stripe and WorldPay are often regarded as easy choices for merchants that want to begin processing quickly, but these solutions can be incredibly picky with the risks they allow on their platforms. With built-in risk and fraud services, these PSPs act as one-stop shops for most of a merchant's payment needs and can help them maintain compliance. However, PSPs of this nature have strict (albeit at times vague) rules that could cause a merchant, especially a higher-risk merchant, to lose access to their payment processing services without warning.

On the other hand, more specialized PSPs like PaymentCloud or Soar Payments have a history of supporting higher-risk businesses and helping them succeed. A specialized PSP may not have nearly as many bells and whistles for merchants but will offer more flexibility for these merchants to choose the fraud and risk solutions that best suit their needs. For smaller merchants with fewer resources, piecemealing services in this way may become cumbersome and ultimately non-viable as an option.

When selecting any PSP, be sure to consider:

- How this partner operates with your designated merchant category code (MCC) and whether similar merchants transact successfully with them.

- The payment methods they offer and whether they meet your customers' expectations.
- What makes this partner unique and a good fit for you, whether they offer fraud prevention, flexibility, performance optimization, global coverage, or reporting you require.
- The level and quality of support you need in a PSP.

While it may be difficult to know which route is the best option for your business, be sure to weigh your company's risks, resources, and growth goals against the PSP options available to you. All-in-one PSPs are notoriously difficult to move away from and while they may provide a means for getting up-and-running quickly, they may not be the best partner long term.

Manage Disputes (Chargebacks)

One of the simplest (albeit not actually easy) ways to remain compliant and operational with both the card networks and any PSP is to keep dispute rates low.

While some disputes may be signs of fraudulent activity (more about this later on), legitimate disputes can occur due to lack of customer support, clarity, or trustworthiness in the brand.

A few ways a merchant can reduce the dispute rate include:

1. **Enhancing transparency and clarity:** provide clear and concise communication with customers throughout the purchasing process. Make sure product descriptions are accurate and detailed, pricing is transparent, and terms and conditions are clear.
2. **Providing prompt customer service:** Offer responsive customer support to address any inquiries or concerns quickly and effectively, and ensure that they come to resolution quickly.
3. **Establish clear return and refund policies:** Clearly articulate return and refund policies in all communications with customers, and make it easy for customers to request and process returns.
4. **Educate customers about chargebacks:** Inform customers about chargebacks and the potential consequences for all parties. Encourage customers to contact you directly with any concerns before initiating a chargeback.

5. **Continuously evaluate and improve:** Regularly review and evaluate your fraud prevention and chargeback management strategies. Identify areas for improvement and make adjustments based on data, trends, and customer feedback.

Reducing legitimate chargebacks and keeping the chargeback rate low can signal to partners that even the riskiest of merchants are safe to do business with.

Work with Trusted Third-Party Partners

While using one PSP may simplify many things for you, this doesn't mean that you shouldn't also work with other partners to keep your high-risk business running. It is especially important when having only a single payment partner that your business has the tools in place to protect itself and remain operational should any major issues arise.

Consider working with third-party providers that specialize in key payments operation areas, such as fraud prevention and payment compliance: this will take difficult work off your plate while keeping your business in the clear.

Fraud Prevention and Management

While merchants could monitor fraudulent activity on their own, this task becomes increasingly cumbersome as processing volumes mount to thousands of transactions or more daily. Many solutions on the market today are especially good at using AI and sophisticated algorithms to:

- Monitor historical performance for trends that could signal attacks
- Identify and flag - and, sometimes, even prevent - suspicious activity in real-time
- Manage disputes as they come in and flag any alarming trends

While these solutions do come at a cost, many merchants consider these to be worthwhile expenses because fraudulent and errant disputes could mean the difference between a smooth running business and one that ceases to operate.

Companies like FraudLabs Pro, Kount, and Feedzai, to name a few, can be seamlessly integrated into a company's payment stack.

Payment Security and Compliance

All-in-one payment processors usually offer a full suite of compliance tools that help merchants maintain secure operations and achieve PCI compliance. However, a merchant using a specialized PSP may have to manage most of this on its own, or select a third-party solution to assist them.

Third-party tokenization providers like Basis Theory can assist merchants that would like to secure their payments, achieve PCI compliance, and maintain ownership over their payments data. These solutions not only take away a significant portion of the burden to maintain compliance, but they also provide freedom in the form of network-agnostic tokens that growing merchants can use with any PSP, partner, or network.

High-Performing High-Risk Merchants

When working in a higher-risk environment, many merchants set their sights on what can keep them operational today. However, by choosing the correct platforms and partners, these merchants can not only survive today, they can also thrive and deliver top-notch customer services while protecting and optimizing their payment systems.

Selecting Multiple PSPs for Optimal Performance

Why Should You Use Multiple PSPs?

To put it simply, leveraging more than one processor in your payments stack can assist in two areas: reducing both risk and fees.

Reduce Risk

Having a single point of failure in any organization is a risky proposition. Using a single payment partner is no different, and by using only a large PSP like Stripe or Worldpay, organizations open the door for many single-point-of-failure issues.

The best way to prevent this risk is to build in a backup payment processor into your payment flow. Should your account close for any number of reasons you'll have ownership over your

payment tokens, meaning you can quickly shift your payment processing to your backup payment processor.

Optimize Fees

Different processors levy different fees, based on the services they deliver. Some will charge more because they are able to handle high-risk merchants, others will charge flat fees in return for a simplified process for payment routing. The reality is that most payment processors are better at some things than others, and that they often have wildly divergent pricing schedules.

As a result, merchants seeking to optimize their payments and their business operations find that implementing a smart payment routing strategy - in which payments are routed to different payment processors, based on an intelligent decisioning process - is a highly valuable option.

How To Select PSPs

Selecting PSP partners is especially important in the high-risk space. And, because it is likely most higher-risk merchants would have to work with a high-risk payment provider, the options may be quite narrow.

For those that have avoided being caught up in the MATCH process, the options may be greater, but the process is unlikely to be easier to manage. This is because every merchant is different, with wildly differing needs, and having the right PSPs in your payment stack can truly set a merchant up for success.

When selecting any PSP to add to your payments stack, be sure to consider:

- How this partner operates with your designated merchant category code (MCC) and whether similar merchants transact successfully with them, or not.
- The payment methods they offer and whether they meet your customers' expectations.
- What makes them unique and a good fit for you, whether they offer fraud prevention, flexibility, performance optimization, global coverage, or reporting you require.
- The level and quality of support - is it what you need in a PSP?

- How well this PSP collaborates with other partners, including PSPs, third-party tokenization providers, fraud management tools, and more.
- What the overlap may be between this PSP and any others you may have, and how this PSP fits into, and enhances, your payment stack.

Optimizing Payments with Partners

PSPs alone are unlikely to offer everything your business will require to continue operating smoothly in the midst of the unpredictable ups and downs of payment processing.

Consider working with third-party providers that specialize in key payments operation areas, such as fraud prevention and payment compliance, that will take difficult work off your plate while keeping your business in the clear.

Payment Orchestration and Smart Payment Routing

When working with multiple PSPs, it is advantageous for merchants to build in sophisticated routing techniques, called smart payment routing, that can ensure the best PSP is selected for each transaction.

Smart routing works by intercepting transactions before the customer's information is sent for processing, and applying an algorithm to known information about the sale to select an appropriate PSP.

For instance, smart routing algorithms may look at:

- **Card issuing country:** to select a PSP with a local presence and higher likelihood to successfully authorize payment
- **Card type:** to select the PSP best suited, for example, to process debit card transactions, which are less expensive overall
- **Card brand:** to select a PSP with the highest likelihood for successful authorization or most agreeable fees, like in the case of American Express cards, which are notoriously expensive to process

Once the routing decision is made, the transaction is packaged up and dispatched to the optimal PSP. If a transaction then fails, a cascading payment strategy may also be implemented to automatically re-present failed transactions to alternative processors in the hopes of arriving at a successful conclusion.

Note: it is important not to be overly aggressive with cascading payments, as sending too many already-failed transactions to a downstream PSP may give partners the impression that your business is (more) risky and could cause them to shut you down.

Solutions like Basis Theory, Feedzai, and Spreedly can provide the flexible infrastructure for merchants to implement sophisticated routing strategies.

Fraud Prevention and Management

While merchants could monitor fraudulent activity on their own, this task becomes especially cumbersome when processing thousands of transactions daily. Many solutions on the market today are especially good at using AI and sophisticated algorithms to:

- Monitor historical performance for trends that could signal attacks
- Identify and flag - and, sometimes, even prevent - suspicious activity in real-time
- Manage disputes as they come in and flag any alarming trends

While these solutions do come at a cost, many merchants consider these to be necessary expenses, because fraudulent and errant disputes could mean the difference between a smooth running business and one that ceases to operate.

Companies like FraudLabs Pro, Kount, and Feedzai, to name a few can be seamlessly integrated into a company's payment stack.

Payment Security and Compliance

While all-in-one payment processors usually offer a full suite of compliance tools, specialized PSPs may not. Many merchants leveraging a multi-processor approach choose to manage compliance through a trusted third-party solution.

Third-party tokenization providers like Basis Theory can assist merchants that would like to secure their payments, achieve PCI compliance, and maintain ownership over their payments data. These solutions not only take away a significant portion of the burden to maintain

compliance, but they also provide freedom in the form of network-agnostic tokens that growing merchants can use with any PSP, partner, or network.

Additional Payment Services

Some merchants may choose to take this even further and work with additional partners that can assist with analytics, subscription management, 3DS, and more. Depending on the nature of your business as a merchant, you may need to work with such partners, or you may opt to take these roles in-house.

Traits of High-Performing High-Risk Merchants

What it Takes to be a High-Performance High-Risk Merchant

As we covered earlier in the series, it can be challenging to operate in a high-risk vertical due to the increased challenges of fraud, scrutiny, chargebacks, fees, and more. Implementing the right strategies, however, can ensure that these merchants not only operate successfully, but also thrive.

Best practices high-risk merchants should follow to become successful include:

- **Understanding industry regulations:** Becoming knowledgeable about the standards that card networks and PSPs have in place regarding chargebacks and disputes, fraud prevention, reporting and compliance, and industry trends can ensure that your business remains operational even as the industry evolves.
- **Choosing the right PSP(s):** Partner with reputable and experienced payment processors that specialize in high-risk merchant accounts and have a history of working successfully with your MCC.
- **Providing clear communication:** Make it easy for prospective customers and partners to understand exactly what your business is, how the purchasing process works, and what the terms of use are. It becomes significantly easier not only for you to fight for yourself in the event of fraud, but also for your partners to do the same.

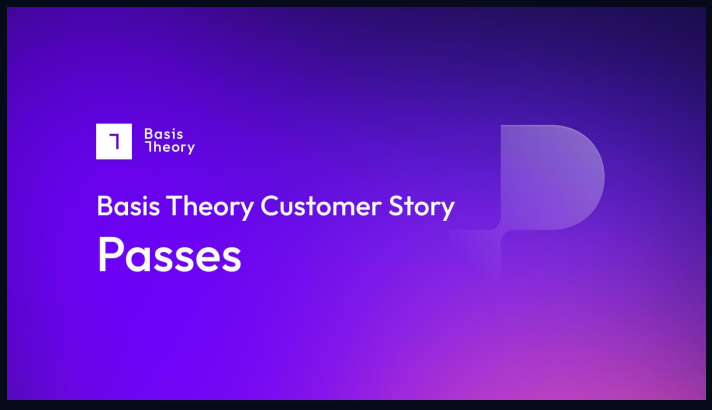
- **Offering best-in-class customer service:** These days, great customer service should be table stakes for most businesses, and especially for merchants in high-risk sectors. Ensure that inquiries into refunds, issues, or general questions are addressed promptly and clearly to keep chargebacks low.
- **Maintaining PCI DSS compliance:** any merchant that handles sensitive card information must be PCI compliant. With several partners in the market that can assist, it is easier than ever to achieve compliance.
- **Monitoring transactions and alerts:** Regularly review transaction data to identify trends, patterns, and anomalies that may indicate potential fraud - and pay close attention to any alerts your payment partners share. High-performing merchants diagnose and address issues before they ever threaten business continuity.
- **Leveraging specialty partners:** Managing payments in a highly regulated environment is not the time or place to DIY or “figure it out”. Enlist trusted partners with expertise to assist with fraud management, compliance, security, and analytics.

Case Study: Passes, a Creator Platform, Thrives with Basis Theory

Founded in 2022, Passes is a Miami-based creator platform that enables fans to access exclusive content and experiences. Passes has a similar business model to OnlyFans or Fansly, empowering creators to monetize on their own by enabling seamless and secure transactions between creators and their fans.

However, the team had trouble building relationships with payment providers because of the perceived high-risk nature of the platform, even with strict content rules that do not allow nudity on its platform. Unfortunately, many PSPs specializing in high-risk transactions were slow, difficult to work with, and could shut them down without warning.

Patrick Zheng, Tech Lead, recalled, "We were working with a PSP, and they said they were okay with our business but they ended up going back on their word and shutting us off without any warning." Passes had to quickly integrate with another payment provider in the middle of the night, but



there was a risk they would be shut down there too. He continued, "We wanted to make sure that we're always in a position where we will have a provider even if something happens."

They found Basis Theory, a PCI-compliant cloud provider for data encryption and storage, through their QSA. The team replaced the front-end component with the Basis Theory card Elements and used the Basis Theory Proxy to send data to PSPs. The implementation process only took two weeks, which was impressive considering how complex PCI compliance is.

By partnering with Basis Theory, Passes was able to build a solid foundation for its payment system, and open the door for cascading payments, ensuring it would always be in a position to have a provider to process transactions for its platform.

Read the entire case study.

How Basis Theory Helps Merchants

Basis Theory can assist high-risk merchants that would like to secure their payments, achieve PCI compliance, and maintain ownership over their payments data. Outsourcing your CDE to Basis Theory not only takes away a significant portion of the burden to maintain compliance, but it also provides freedom in the form of network-agnostic tokens that growing merchants can use with any PSP, partner, or network.

Resources to Continue Learning about High-Risk Payment Processing

It is no secret that the payments industry continues to evolve at a rapid pace; keeping up with the industry news, trends, and best practices can be challenging.

Basis Theory Resources

Our payments experts have written several articles tailored to high-risk merchants.

High-Risk Merchant Category Codes (MCCs) - Learn more about the rules credit card associations place on particular "higher risk" MCC categories for risk monitoring.

What Are High-Risk Payment Processors? - Oftentimes, high-risk merchants must use specially designated payment processors that specialize in their business. Learn why.

What is a High-Risk Merchant & How Do Payments Work? - Learn more about what it means to be a high-risk merchant and how this impacts payment processing.

All parts of this series:

- The Rules of the Game
- How Are Merchants Shut Down?
- How to Stay Operational with 1 Payment Processor
- Working Effectively with Multiple PSPs
- High-Performing High-Risk Merchants: Best Practices

Other Great Resources

Other great resources merchants can use to stay knowledgeable about the high-risk industry include:

- PayPod - a podcast by Soar Payments that discusses payments, fintech, and technology.
- Aeropay blog - this blog offers helpful business advice for merchants operating in high-risk industries
- Zen Payments blog - this blog offers valuable tips for anyone transacting high-risk payments
- Ultimate guide to high-risk merchant accounts - Durango Merchant Services authored this excellent guide