Infinicept
GET PAYMENTS GOING YOUR WAY™

Compliance 101

Payment facilitators – also known as Payfacs® – are obligated to follow rules and regulations from the multiple entities that govern the payments ecosystem. Compliance is achieved by implementing the appropriate processes needed to adhere to these rules and remaining aware of changing conditions.

Who Regulates Payment Facilitators?

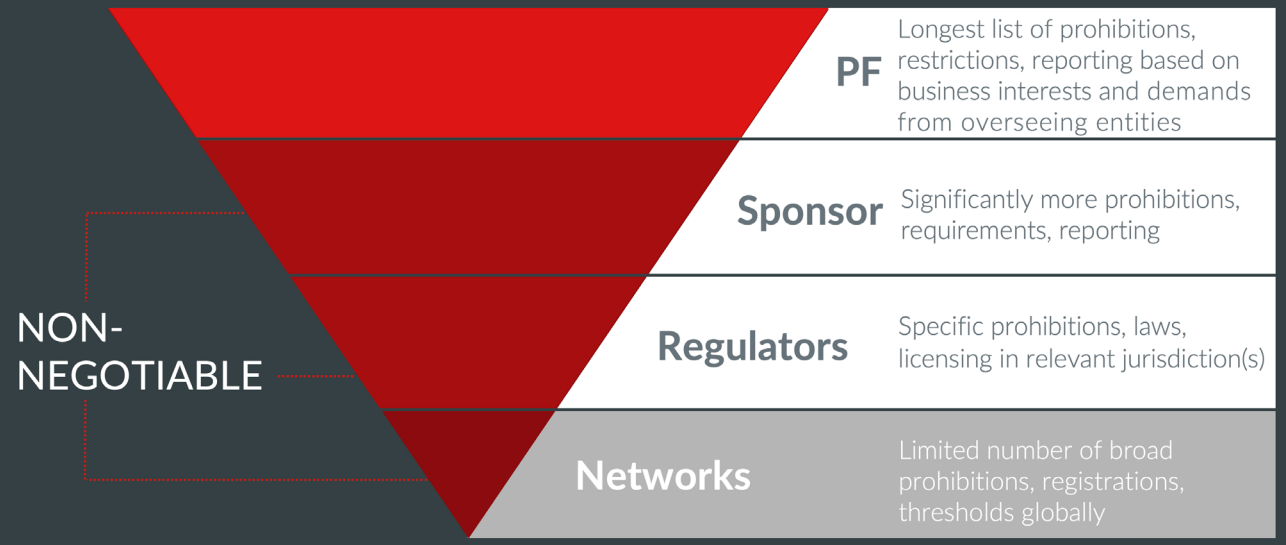
The short answer: everyone. Everyone, that is, with a role in regulating the payments industry.

As a Payfac, you are subject to the requirements of all of the entities above you in the payments ecosystem. This includes state and federal government regulators. It also includes the card networks (primarily Visa and Mastercard), which maintain sets of rules that apply to all of the entities connected to the card payment ecosystem.

And finally, it also includes the acquiring banks that sponsor Payfacs. In the Payfac model, Payfacs are the entities that have direct relationships with their merchants. This means that banks will often pass down their payment-enabling responsibilities to the Payfacs they sponsor. At the same time, sponsoring banks are allowed to design their own requirements or limitations for the Payfacs they enable. You'll be responsible for adhering to all of the rules laid out by your own individual sponsor or sponsors.

As a Payfac, you are also free to design your own rules that are more conservative or restrictive than the requirements that are placed on you. They cannot, of course, be less restrictive than what the parties above you mandate.

Regulatory and Compliance Demands



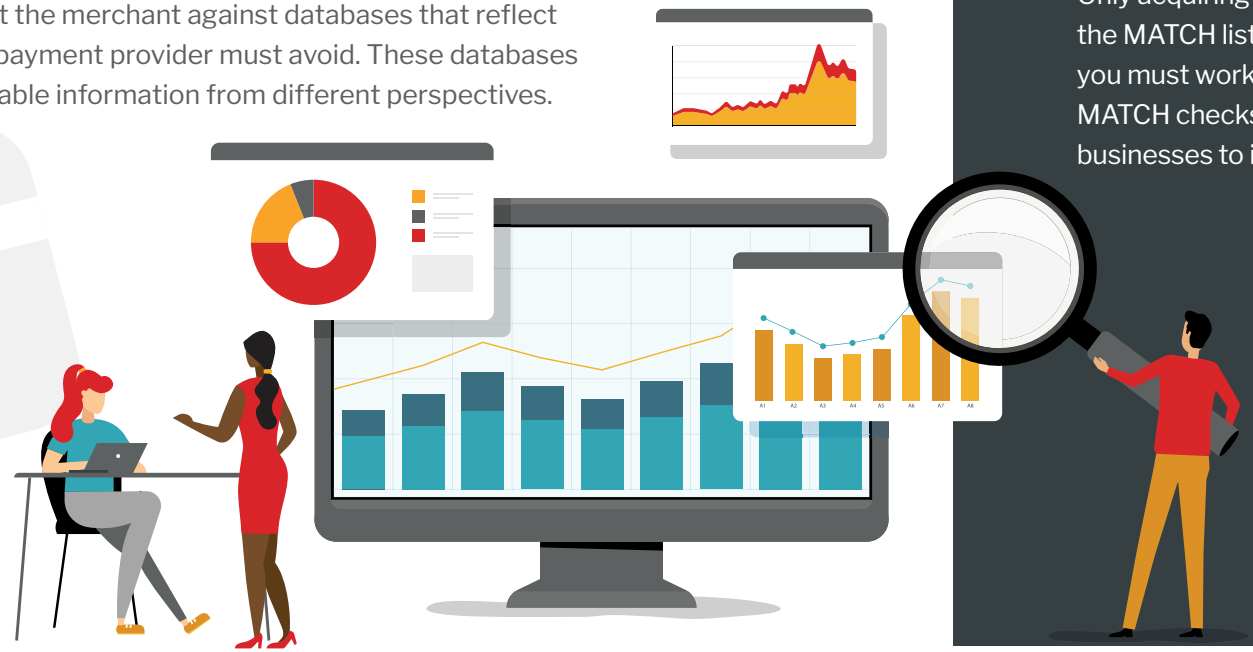
What are the Primary Requirements?

While not a comprehensive list, this section covers many of the requirements that apply to most Payfacs. Every Payfac is responsible for knowing any rules that apply specifically to them.

UNDERWRITING / DUE DILIGENCE CHECKS.

Underwriting and initial merchant assessments are required of all entities provided access to the payments system. Before onboarding merchants, all payment providers (Payfacs here) must conduct due diligence on those businesses and the individuals behind these merchants to verify their identities and to guard against fraudulent or criminal activity. As a Payfac signing up submerchants, these requirements now apply to you.

One of the pieces of this puzzle involves checking the details known about the merchant against databases that reflect entities the payment provider must avoid. These databases provide valuable information from different perspectives.



MATCH (card networks)

Mastercard hosts a database called Member Alert to Control High-Risk Merchants, commonly referred to as the **MATCH** list. The card networks mandate that acquiring banks screen potential merchants and their principals against this list of entities. Businesses or individuals on the list have been associated with problems within the payments networks and been terminated by their acquirers in the past.

Acquirers also must ensure that any merchants they or their Payfacs terminate are added to MATCH if the listing criteria are met.

Only acquiring banks have direct access to the MATCH list via Mastercard, so as a Payfac, you must work with your acquirer to run the MATCH checks, as well as to add individuals or businesses to it as appropriate.

Office of Foreign Asset Control (OFAC) list of prohibited merchants (U.S. Treasury Department)

The government operates multiple lists of prohibited merchants, but they're often referred to in aggregate as the **OFAC list**. As a payments provider, you must screen your portfolio against these lists, verifying that the merchant and its principals or owners are not on it.

You must also re-run this check periodically (monthly at minimum), to scrub your portfolio of any existing merchants that have been placed on it. The screening is often run by the acquirer as well, but the Payfac has first-line responsibility.

ONGOING MONITORING AND REPORTING

In addition to performing due diligence on your merchants before allowing them into the system, you must also perform ongoing monitoring of your portfolio and merchant activity once you're processing their transactions.

Suspicious Activity Report (SAR) Filing (Sponsor-specific, required of payments providers by federal government)

Your acquirer (or sponsor bank through your acquirer if the acquirer itself is not a registered financial institution) is required to report on certain activity under the Bank Secrecy Act (BSA) using Suspicious Activity Reports (SARs).

Some acquirers push this requirement directly down to their Payfacs. Others file SARs themselves, requiring their Payfacs to provide them with the information necessary to determine whether a SAR should be filed. Some acquirers may also require Payfacs to file continuous activity reports, while others do not. No information regarding the filing or potential filing of a SAR may be disclosed to the individual or merchant.

Brand-required Transaction Monitoring (Visa)

Visa requires a minimum level of traditional transaction risk monitoring. You could design your own monitoring to add more. Examples of things to monitor for include the following. (See the Visa GARS guide for the full requirements):

- Unsettled authorizations
- Excessive keyed transactions
- Outside of approval parameters
- Forced sales
- Prepaid card
- Same BIN
- Same card across portfolio

Chargeback monitoring (Visa / Mastercard)

The card networks set thresholds for allowable numbers of chargebacks generated by any given merchant. For Payfacs, the goal is to identify chargeback-inducing merchants early, before reaching the thresholds set up by the card networks. Reaching the thresholds will generate fines and reprimands from acquirers. While the thresholds differ between networks and can change, a basic rule of thumb is that around 100 basis points worth of chargebacks will trigger action from the networks, but Payfacs should have monitoring and processes in place to identify and take action upon merchants long before they reach that level.

Reporting Requirements (Card networks / sponsors)

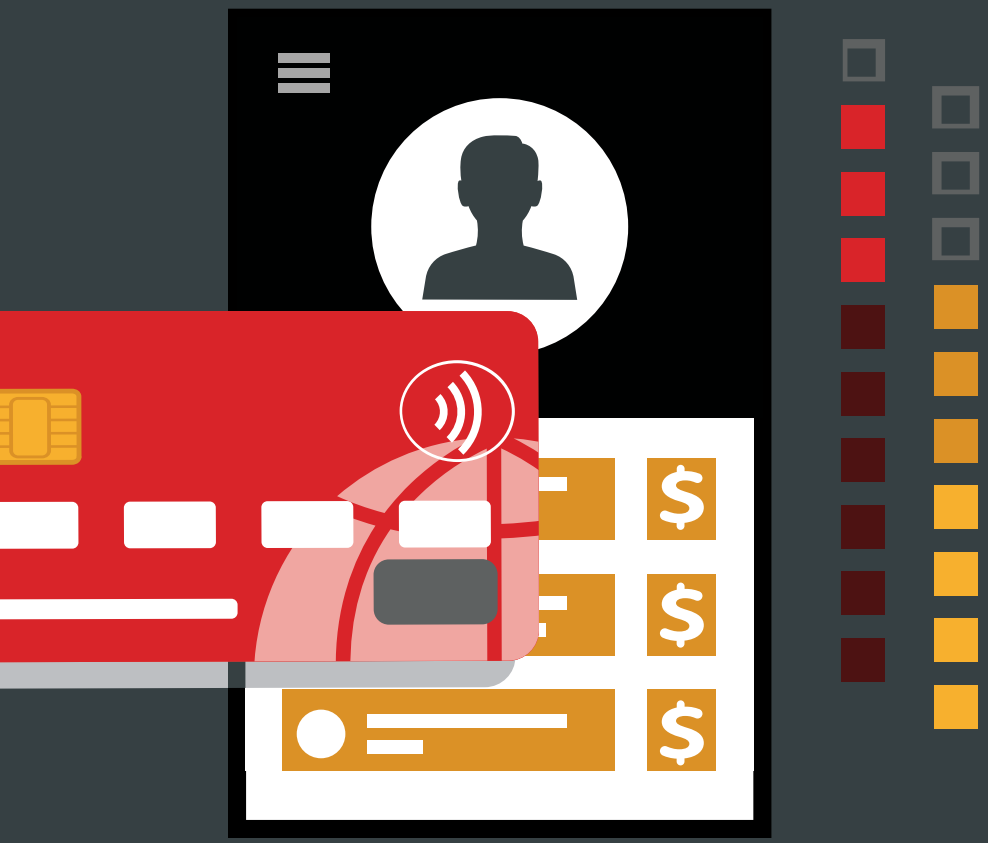
There is a certain level of insight that you must have into your portfolio, either for your own management of your portfolio, or to provide to card brands or your acquirer when they request it. Depending on the information you provide in your transaction messages, reporting could be requested on a quarterly basis.

This means you must be able to track certain information segmented by portfolio, merchant category code, agent, and submerchant. This information includes things like:

- Sales dollar volume
- Number of sales
- Refund dollar volume
- Number of refunds
- Chargeback dollar volume
- Number of chargebacks
- Reject EFT amount
- Reserve amount

PAYMENT FACILITATOR PROGRAM REQUIREMENTS

The card networks have certain requirements for their Payfac programs specifically. You must adhere to these requirements in order to operate as a compliant Payfac.



Volume thresholds

If a submerchant processes $1,000,000 USD or more in Mastercard or Visa volume, that submerchant must a) have an agreement that includes the acquiring bank (rather than just the Payfac alone) and b) receive funding directly from the acquiring bank. Visa has made changes to this rule to allow for certain submerchant relationships to be exempt from this rule, while Mastercard retains this requirement in all submerchant instances.

Prohibited submerchants

There are certain segments of merchants in the payments industry where Payfacs are not allowed to operate. Payfacs are prohibited from aggregating other Payfacs, as the practice obscures who the true merchant really is. They are also prohibited from serving:

- Internet gambling in jurisdictions where the practice is illegal
- Merchants on MATCH
- The sale of any goods or services that purport to test, cure, treat, or prevent COVID-19
- Staged digital wallets

Registration

Payfacs may be sponsored into the card networks by one or more acquiring banks, but are required to register with each they work with before being allowed to go live with transactions through that acquirer. Each different type of business model (ISO or Payfac, for example) is separately registered – being registered as one doesn't cover you for others.

Registration fees are per acquirer / sponsor and debited directly from the Payfac's operating account. The more acquirers you work with, the more annual fees you will see. Mastercard registration is $3,000 USD annually, and Visa registration is $5,000 USD annually. There is also a Mastercard discovery fee of $9,000 USD that will be assessed to an acquirer if the network finds that it is supporting a Payfac that is operating but not properly registered.

The Payfac must receive a written confirmation of registration prior to running transactions.

Training requirements

Payfacs must train and provide education and updates to their underlying submerchants. Card brands have direct relationship with acquirers, but not with you or your submerchants. They require acquirers to pass down their training directly to Payfacs, who pass it down in turn to their submerchants.

Transaction message / unique identifier requirements

As a Payfac, you receive a business identifier from the networks when your sponsor registers you. You or the acquirer also, most commonly, provide individual submerchant IDs. These identifiers must be used in transaction messages according to requirements from the card networks.

HIGH-RISK REGISTRATION

Payfacs operating in high-risk industries are subject to rules and requirements above and beyond those of regular Payfacs. If your sponsor allows you to work with merchants in certain merchant categories that are considered high-risk, you are considered a high-risk Payfac, and your acquirer is a high-risk acquirer.

This designation comes with additional cost and oversight. Some sponsoring banks will simply prohibit Payfacs from operating in high-risk industries for that reason.

Card-Not-Present Merchant Types Requiring High-Risk Registration

- **MCC 4816,** High-Risk Cyberlocker Merchants, Computer Network/Information Services (Only for the Sale of Access to Cyberlockers or Remote Data File-Sharing Services)
- **MCC 6051,** Cryptocurrency Merchants
- **MCC 6211,** High-Risk Securities Merchants
- **MCCs 5967 and 7841,** Non-Face-To-Face Adult Content and Services
- **MCC 7995,** Non-Face-To-Face Gambling Merchants, Digital Goods-Games (Daily Fantasy Sports as example)
- **MCC 5122 and 5912,** Non-Face-To-Face Pharmaceutical Merchants
- **MCC 5993,** Non-Face-To-Face Tobacco Product and ENDS (Electronic Nicotine Delivery Systems) Which Include E-cigarettes, Vape Pens, And Cartridge Merchants
- **MCCs 5122 and 5912,** Drugs, Drug Stores, Pharmacies (but only if conducting non-intra country transactions)
- **MCCs 5962, 5966, and 5967,** Direct Marketing (Inbound or Outbound or Travel Related)
- **MCC 7273,** Dating and Escort Services

PCI DSS COMPLIANCE

The Payment Card Industry Data Security Standard, known widely as PCI DSS, was developed by a coalition of five card brands (American Express, Discover, JCB, Mastercard and Visa) to protect the integrity of the payments system. Any entity that stores, processes* or transmits cardholder data – including payment facilitators – must comply with the standard.

Requirements for service providers, including Payfacs, are divided into two levels (Level 1 and Level 2) based on the number of card transactions they process. Merchants have four levels of requirements.

Payfacs must complete a self-assessment questionnaire (known as SAQ-D certification) and provide Level 1 or Level 2 attestation to their sponsor bank on an annual basis. Payfacs are also responsible for making sure their submerchants are PCI compliant.

These steps mean that all entities across the payments ecosystem have the same level of security and can attest to that to their partners. You also have the right to request an attestation from your own partners.

PCI requirements update to new versions periodically, with a transition year to allow people to assess against the older version while they transition to the new version.

* Processing means the processing of data. Anywhere data flows through business processes, in electronic or hard copy, would be in scope. The only place not in scope is where connectivity is provided. Networks are not in scope, but the entities on both ends would be.

Steps to ensure PCI compliance

1. Understand what you need to do to achieve and maintain compliance. The PCI website is a great resource for information and training, and there are companies, like ControlScan and MegaplanIT, that can advise you.
2. Consider the amount of customization and control you want to have over the customer experience. A more individualized user experience may result in larger compliance scope. Less control can bring less revenue but also smaller scope and, subsequently, lower risk.
3. Use a gateway and token vault so you never store sensitive data. Firms like Very Good Security (VGS) provide solutions that give you control and flexibility.

Conclusion

As companies that are enabling access to the payments system, Payfacs are responsible for protecting its integrity. That's why compliance with industry rules and regulations is critical – and required. Plenty of resources are available, and ongoing education, communication, and industry participation are key to successfully adhering to industry requirements.

To speak with a compliance expert or to learn about how Infinicept can help you better understand the world of compliance, contact us.