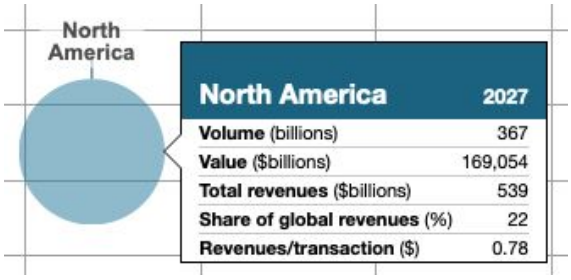
The Risk Factor: What to Consider when Becoming a Payment Facilitator

The movement of B2B software companies and digital marketplaces toward payment facilitation is one of the most discussed topics in the payments industry today. And for good reason: as outlined in previous white papers, the path to payment facilitation can afford these SaaS companies increased revenue, better control over the customer experience, and increased total enterprise value. Companies need look no further than the blueprints for PayPal, Square, Stripe and Shopify, whose payments revenue eclipsed recurring subscription revenue in 2016 and has shown no signs of slowing.

In addition to this upside, many software companies are feeling the push to payment facilitation from their owners/investors – many times venture capitalists and private equity firms. Not only are these VCs and PE firms pushing their portfolio companies, they are also investing in the technology that facilitates becoming a payment facilitator.

In fact, Boston Consulting Group's Global Payments: The Interactive Edition predicts that by 2027, software companies will represent $154 billion of North American payment revenue[1]. For all these reasons and more it seems like a no-brainer to leverage the payments experience to earn more revenue.



But making the move to becoming a payment facilitator doesn't come without some risks. Afterall, becoming a payment facilitator means your software company becomes a payments company - and owns all the risk that comes with it. This white paper outlines those risks and puts into perspective the importance of understanding risk in the payments space.

With the revenue generating opportunities and increased valuation, it is easy to overlook the subject of risk in this strategic business decision. While some in the industry frame the consideration as easily solved with a tech stack and nominal staff investment, we believe the subject of risk must be at the forefront of the considering this decision. Here are the most important questions that your company should be be prepared to answer pertaining to risk:

1. **How much are you willing to invest in infrastructure to develop a platform to manage not only the payments business, but also the tools and experience to manage risk?**
2. **What will your risk appetite be?**
3. **Do you have the risk and compliance expertise to build policies, procedures and processes that comply with requirements mandated by regulators, card networks and sponsor banks?**

Here is a deeper look into why these questions are so important as it pertains to risk.

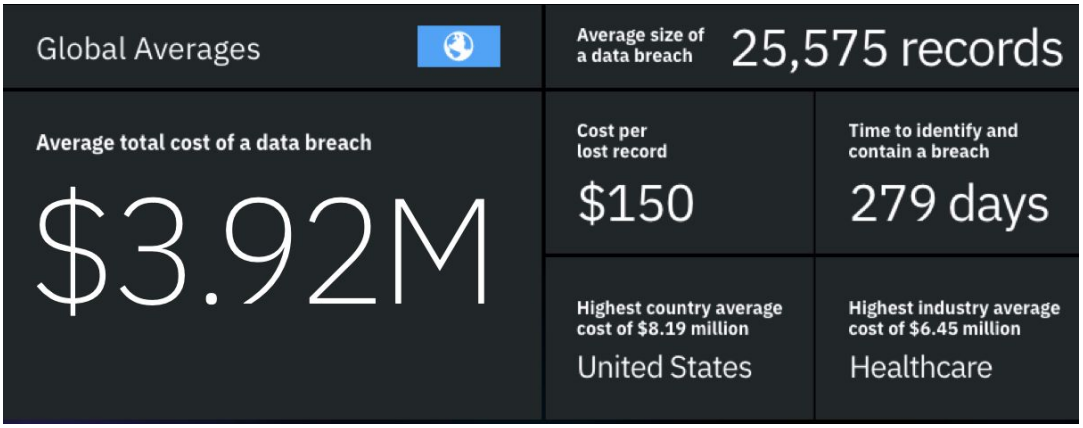
Risk – What is it?

In the digital payments age, risk management is such a complex, interconnected and vast topic that software companies and payment facilitators must deeply understand it in order to protect their company from financial and reputational loss. Here's a broad definition that we'll start with: Payment risk is the risk of loss due to a default on a contract, or more generally, the risk of loss due to some "payment event."

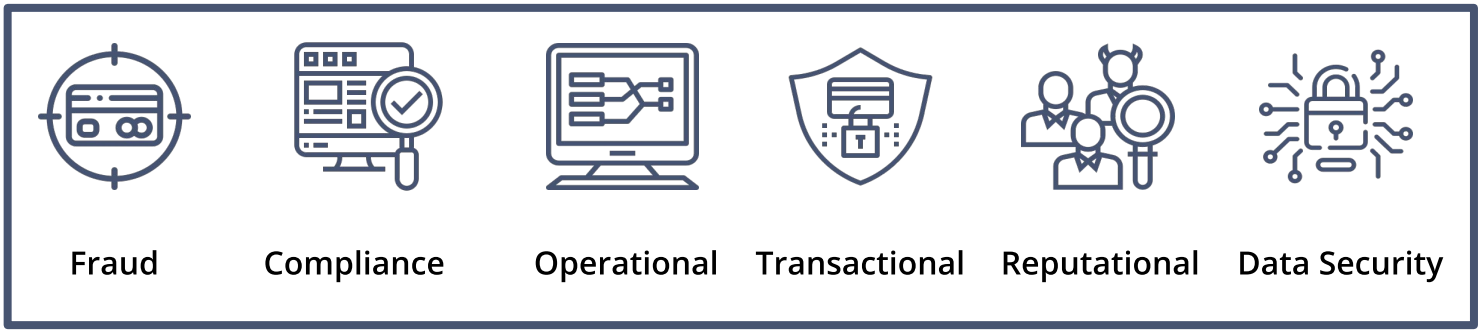
It is important to remember as a payment facilitator you are accountable to sponsor banks, card networks (Visa, Mastercard, Discover, American Express), government regulators and your acquirer to control who is on the platform, meet several governmental agency requirements, be able to audit and reconcile account activity on your platform and become and maintain PCI compliance (for you and your merchants.)

As pressure to grow revenue potentially leads to expansion in international markets it's also important to understand the increased complexity to manage risk globally. According to a recent Global eCommerce Expansion Payments and Fraud Prevention Trend Report by Internet Retailer, the number one barrier or obstacle to sell to online shoppers in other countries is fraud prevention. The report states, "many online retailers are wary of the complexity and expense of handling payments in foreign currencies, and the added burden of accepting payment methods not common in North America[2]."

Handling sensitive payment data also poses potential financial risks. According to the 2019 Cost of a Data Breach Report by Ponemon Institute, the average cost of a data breach in the US is $3.92 million. According to the same report, the average size of a data breach is 25,575 records but there have been several in the millions including Adobe, 7.5 million records, Capital One, 106 million records, and Zynga, 218 million records[3].



As a payment facilitator you will be taking on many of the responsibilities that once fell on the shoulders of an acquirer. One of the major responsibilities is to understand and manage risk. To better understand the complexities of risk, we've broken it down into the following six categories with a deeper dive:



Fraud

Payment fraud (we'll just refer to as fraud) is any type of illegal transaction completed by a criminal. This may include unauthorized transactions, stolen merchandise, or false requests for refunds through methods like phishing, identity theft, account takeovers and stolen payment credentials.

Some recent trends that are affecting fraud include:

- Consumer demand for remote purchasing (i.e. mobile shopping)
- Continued adoption of EMV in the retail environment driving fraudsters online
- Increase in digital goods being sold online
- Increase in volume of international transactions

Online payments fraud

Payments fraud can take many shapes, including:

Identity theft – is the most common type of eCommerce fraud and the hardest to detect. It most often occurs when a criminal uses stolen card data which may be obtained through the dark web, or by convincing buyers to purchase on fake websites, or other deceptive techniques. This was recently described as "clean fraud" because it is very difficult to detect, and the transaction seldom gets flagged or blocked by automated systems.

Phishing – often occurs via email when the criminal asks for user IDs, passwords, credit card information or other personal information. The emails will often emulate a financial institution or internal co-worker and can look like legitimate requests.

These represent just a few of the schemes that online fraudsters use to commit fraud. Stealthy and constantly finding new ways to commit fraud online, these individuals do their best to stay one step ahead of the technologies, systems and processes used to protect the payments ecosystem.

Retail payment fraud

The good news is that retail payment fraud is being reduced, but unfortunately this means criminals have migrated online to conduct fraud. Below are two key areas to have on your radar:

Stolen credit cards – buying products and services with a stolen credit card is quite simple and has been in existence since the first credit cards were issued.

Counterfeit cards – in September of 2019 Visa reported that chip cards have reduced counterfeit fraud by 87%[4], however it still happens from time to time.

Today's brick and mortar retailer will typically sell through physical storefronts and have an online presence, so although fraud in the retail environment is going down, it is gaining momentum online. Widespread adoption of EMV, new payment options (wallets), the growth of international transactions and more sophisticated hackers have caused an increase in eCommerce fraud. According to Juniper Research, in 2020 online merchants are expected to see 65% of all fraud value[5].

Friendly Fraud

Friendly fraud occurs when a real customer orders a product online and receives the goods or products, but claims they did not receive them and files a chargeback with their bank rather than asking for a refund through the merchant.

A chargeback refers to the act of returning funds to a consumer who has purchased a product or service from you. The refund itself is returned by the merchant but is handled and processed by the credit card issuer. The concept of chargebacks exists to protect the consumer, but sometimes dishonest consumers can make false claims. Chargebacks can take place in both online and in-person environments.

Chargebacks have ramifications for software companies that become payment facilitators especially for your end merchants (or sub-merchants). Every time a consumer files a chargeback, fees are levied on the merchant. Too many chargebacks (over a certain threshold) can result in termination of the merchant account. If you are providing processing, settlement of funds and billing your merchants, you will be responsible for handling chargebacks.

The 2019 True Cost of Fraud Retail Study by LexisNexis found that the cost of each dollar of retail fraud losses is up 6.5% from 2018. For every dollar of fraud, a merchant will pay $3.13 in related expenses for things like chargebacks, investigation costs, legal fees, IT and security costs[6]. Juniper Research indicates that online sellers alone will lose $130 billion to online payment fraud between 2018 and 2023[7].

It is safe to say that payment fraud, whether online or in a retail environment is a risk that every payment facilitator must understand and be willing to take on.

Compliance

One of the core benefits of the payment facilitator model is the ability to quickly underwrite and board merchants - commonly referred to as frictionless, instant or flexible boarding. Whereas a traditional acquirer might take 3-5 days and have 150 questions on the application, a payment facilitator will have considerably fewer questions and have a sub-merchant processing payments in minutes or hours.

Regardless of how fast and frictionless a sub-merchant can be boarded, there are government and regulatory requirements that must be met. A payment facilitator is responsible for who is on the platform, and must have approved processes and procedures in place to prove this to their acquirer.

The payment facilitator must ensure that their sub-merchants are covered for money laundering, terrorist financing and all other risks. This includes meeting KYC (know your customer), AML (anti-money laundering) and OFAC (Office of Foreign Asset Control) requirements. Most of these are enforced by the card networks and acquiring banks but as the payment facilitator, managing them becomes your responsibility. In many cases, each bank or card brand has different rules, creating an intricate web of compliance requirements.

KYC – is an abbreviation for "Know Your Customer" and refers to either the government regulations or the policies, procedures and technologies used by financial services companies to prevent money laundering, financing terrorism or other criminal activity involving the movement of money.

During the underwriting process, a payment facilitator is required to identify the business owner(s) according to rules and regulations set by the US Patriot Act, Bank Secrecy Act, AML laws and FinCEN (Financial Crimes Enforcement Network). According to FinCEN rules, the payment facilitator must validate the identity of any individual that owns 25% or more of the business entity – these individuals are known as beneficial owners[8]. Additional rules and regulations may apply to other business types, such as high-risk merchants.

AML – is an abbreviation for Anti-Money Laundering and refers to laws and regulations that attempt to prevent fraudsters from disguising illegally obtained funds as legitimate.

OFAC – is an abbreviation for the US Office of Foreign Asset Control which is a department of the US Treasury that enforces economic and trade sanctions against individuals, groups of individuals and countries involved in terrorism, drugs and other activities.

As a participant in the payments ecosystem, you are required to ensure that your sub-merchants and their respective beneficial owners are not on the OFAC list or any other global sanction watchlist.

And if operating internationally there are additional government regulatory bodies to consider. For example, Canada has its own equivalent to the OFAC called OSFI – Office of the Superintendent of Financial Institutions.

As the payment facilitator taking on the financial risk, you are also responsible for determining the sub-merchants financial viability during underwriting, which includes obtaining a credit score and conducting an EIN/TIM match.

Card Brand Compliance

The four major card brands (Visa, Mastercard, Discover and American Express) have rules and regulations that any business accepting credit cards must adhere to. Each of these card networks regularly update and publish their respective rules and regulations. Not only must payment facilitators adhere to these rules and regulations, but they must also require their sub-merchants to adhere as well.

Generally speaking, the payment facilitator must ensure their sub-merchants do not engage in any illegal activity; fraudulent, deceptive or unfair business practices; or sell goods and services that are prohibited, like adult digital content or gambling services. It is also the payment facilitator's responsibility to ensure that each sub-merchant has policies for returns, refunds, customer service, and other disclosures in accordance with the card brand operating rules and regulations.

Below are links to the card brands where you can find information about each program.

WWW.VISA.COM/CISP

WWW.MASTERCARD.COM/SDP

WWW.DISCOVERNETWORK.COM/DISC

WWW.AMERICANEXPRESS.COM/DATASECURITY

PCI Compliance

The Payment Card Industry Data Security Standards (PCI DSS) are requirements created to ensure that all companies that process, store or transmit credit card information protect the cardholder data. The requirements are administered and managed by the Payment Card Industry Security Standards Council (PCI SSC) which is a non-governmental body created in 2006 by Visa, Mastercard, American Express, Discover and JCB. There are over 1,800 pages of official documentation and 300+ security controls in PCI DSS.

PCI DSS compliance includes three main areas - handling card data, storing data securely, and annual PCI DSS validation.

All merchants must meet PCI DSS requirements but payment facilitators have additional responsibilities. Because they process, store and transmit cardholder data for a third-party (i.e. their sub-merchants), they must register with the card brands as a Level 1 PCI DSS Compliant Service Provider. This requires the payment facilitator to perform an annual independent security audit and complete ongoing network vulnerability scans performed by an Approved Scanning Vendor (ASV).

Since all merchants must meet PCI DSS requirements, the payment facilitator is ultimately responsible for ensuring their compliance – even if the payment facilitator itself is compliant. Failure to meet PCI DSS requirements can lead to fines, higher transaction fees, and/or the termination of the contract between the card brand and the payment facilitator or submerchant.

There are also obligations required by the PCI SSC and individual states if the sub-merchant or payment facilitator suspects or validates there has been unauthorized access to their system, and/or use or theft of cardholder information.

More detailed information about the PCI DSS requirements are in the Data Security section below.

GDPR – General Data Protection Regulation

GDPR was agreed upon by the European Parliament and Council in April 2016 and became effective May 25, 2018. It is the primary law that regulates how companies protect EU citizens' personal data. The regulation contains 11 chapters and 91 different articles. A few of the key privacy and data protection elements are:

- Requiring the consent of subjects for data processing
- The right to be forgotten
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

In addition to EU members, any company that markets and/or sells goods and services to EU residents, regardless of its location is subject to the regulation. If a payment facilitator or your sub-merchants collect any of the regulated data from a European user you must be GDPR compliant.

GDPR protects things such as names, addresses, web data, health, biometric, racial, and ethnic data and takes a wide view of what constitutes personal identification (PI) information. Companies must treat things like IP addresses and cookies the same as they do names and social security numbers.

Two types of companies must comply with GDPR – data controllers and data processors. GDPR places more requirements on data controllers as they are the owners of the data. Article four of the requirement defines them as below:

Data Controller – "controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor – "processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

A common example used to explain the difference is a seller of widgets to consumers versus the email automation company they leverage to send emails. The seller of widget is the data controller and the email automation company is the data processor

GDPR fines have been designed to make non-compliance a very costly mistake for large AND small businesses. The data protection regulators in each EU country will determine whether a fine will be assessed and how much the fine will be. There are two tiers of GDPR fines which are as follows:

Less Severe Infringements – fines up to 10 million Euros or 2% of the company's worldwide revenue from the preceding year, whichever amount is higher.

More Severe Infringements – fines up to 20 million Euros or 4% of the company's worldwide revenue from the preceding year, whichever amount is higher.

Operational Risk

Operational risk is the risk of loss from inadequate or failed internal processes, procedures, systems and/or employees. Operational risks can be broken down into the following categories:

Technology disruptions – cyber- and/or physically- disruptive threats to networks, malware, employee error, as well as old hardware failures that can cause risk to a payment facilitator. These technology disruptions can be to your own software or hardware, as well as that of your vendors/partners.

Outsourcing – or third-party risk is the potential risk that arises when a company relies on outside parties to perform services. In the payment facilitator model, outsourcing at least some payment functions occurs in nearly all cases.

Talent/Staffing Risk – describes the struggle to attract, train and retain top talent in roles for payments and software development (e.g. coders, developers, etc.). This can lead to less-experienced workers being pushed into high-pressure roles.

Organizational Change – the risk resulting from adding payments to your technology stack and the accompanying organizational change – from integrating it, to marketing and selling it. These organizational changes can lead to disruption and risk in your company.

Transactional Risk

Transactional Risks are those that can cause loss related to the actual processing of a transaction or the inherent risk in the portfolio of sub-merchants.

Transactional Risk and Risk Monitoring – as a payment facilitator you are required to monitor your sub-merchant transaction activity for anything that deviates from the normal or expected behavior. It is your responsibility, as the payment facilitator, to control your portfolio of sub-merchants' risk. Control at the sub-merchant level may mean the need to institute processing caps, delay funding or create reserves.

A few examples of transactional activity to monitor for include:

- Transaction amounts that significantly differ from the normal average ticket amount
- Large spikes or declines in transaction volume
- Unusual amounts of refunds and/or chargebacks

Credit Risk – typically this is viewed as a risk for banks and is related to loans or an extension of credit (mortgages, loans, credit cards, etc). Payment processors and therefore payment facilitators, take on credit risk (a line of credit) because they often settle a transaction with a merchant before the goods are delivered. If they attempt to collect funds from a merchant for a chargeback and that merchant has gone out of business, the payment facilitator will be held liable thus creating a credit loss.

Reputational Risk

Reputational risk describes the potential for negative publicity having an adverse effect on revenue, market share and/or public perception.

There are specific reputational risks (bad customer service, CEO scandals, etc.) inherent in merely running a business, but we'll focus more on potential reputational issues related to payment processing. Although reputational risk can be subjective, one wrong or bad step in today's instant news cycle and social media dominated world can be tremendously magnified and spread quickly out of control.

As previously outlined, it is your responsibility to "know your customer" so in cases where the sub-merchant is involved in illegal or immoral activity (although obviously not disclosing it), you as a payment facilitator are still responsible. If you board a merchant with inactive website domains that upon approval activates these domains without your knowledge and you process transactions, you have yet another risk to address.

And the types of merchants that you board can be problematic even if they are not illegal per se. A few examples of potentially problematic products/services include:

- Hate Speech
- Drug Trafficking (often get approval as legitimate merchants)
- Massage Parlors (often fronts for illegal prostitution and human trafficking)
- Psychic Merchants (often leads to a large number of chargebacks)
- Firearms
- Vaping Products
- Multi-level Marketing

Beyond the types of merchants and potential for illegal and immoral activity, there are other elements of processing payments that can negatively affect your reputation. One prime example is keeping personal information or PI secure. Although data breaches have become common and are unfortunately regularly reported on today, your reputation as a player in the payments ecosystem could be negatively affected. Data breaches caused by skilled hackers are just one of the ways in which data can be compromised. You are just as likely to be comprised by things like paperwork being thrown into a dumpster, losing a laptop or USB drive or having someone break into your office and steal information.

In addition to customers, getting on the wrong side of the regulators, card brands and acquirers can also create lasting damage to your reputation.

Data Security

According to a Clark Howard report, there is a new victim of identity theft every 2 seconds in the United States[9] and Experian reports that 31% of data breach victims later experience identity theft.

At least 5.3 billion records[10] that include credit card numbers, phone numbers and other highly sensitive information were exposed in 2019. No industry seems to be immune to hacker's efforts as retailers, restaurants, insurance companies, financial services companies, online marketplaces, and health care companies have all fallen prey to data breaches.

Although it seems people have become desensitized to the news about data breaches, protecting data has become even more important as stricter regulations like GDPR are being implemented across the globe.

PCI

According to the PCI DSS Requirements and Security Assessment Procedures, "PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to ***all*** entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to ***all*** other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)[11]."

Their published high-level overview includes the following 12 requirements.

Build and Maintain a Secure Network and Systems	**1**	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3**	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5**	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7**	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data

Regularly Monitor and Test Networks	**10**	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	**12**	Maintain a policy that addresses information security for all personnel

Validation and enforcement of compliance are not performed by the PCI SSC but rather by the processor or facilitator themselves. Each has incorporated the requirements into their own respective data security compliance programs.

It is in the best interest of any business that is processing cardholder data to ensure that they are following the PCI requirements and have internal processes and procedures in place to securely handle personal information. There is a real threat of data breaches but this also will protect against accidental or employee errors.

Not complying with the requirement could lead to:

- Monetary loss from fines and penalties
- Termination of ability to process payments
- Damage to your reputation

The work isn't over once you become compliant. You must maintain compliance through assessments and audits. The assessments and level of security will differ by size of merchants. You should refer to your acquirer for details on PCI DSS compliance.

There are at least two technologies that can help reduce the scope of PCI DSS requirements.

Point to Point Encryption – a point-to-point encryption solution is comprised of hardware (point of sale device) and software (encryption, decryption, key management, etc.). Leveraging a PCI point-to-point encryption solution will subject you to fewer PCI DSS requirements and potentially save your company time and money.

Tokenization – a solution that converts a card number into a numeric code that is used during the transaction. This code is irreversible and has no value if stolen. The customer's real data is therefore protected and can't be intercepted during a transaction. Tokenization also improves data security and reduces PCI DSS scope and costs.

Conclusion

As previously described, there are significant and meaningful reasons to become a payment facilitator, including more revenue, higher valuation, and better merchant experience. However, as we've outlined in this white paper, there are also a number of risks that should be taken into consideration. The balance between revenue upside and risk aversion varies by organization and should be carefully considered by your company's management team.

A few other considerations include:

- Having the available capital to build a payments company
- Adding headcount with payments experience (especially related to risk and compliance)
- Being dedicated to operating and maintaining a payments company
- Having the volume of transactions to justify the expense
- Having the right type of client base for the payment facilitator model

Managing the transition from simply being a software company to also being a payments company, and the accompanying risk of being a payment facilitator may at times seem daunting - but with proper understanding, planning, technology and expertise - the management and ownership of that risk unlocks the financial benefits and promise afforded by controlling payments.

Sources:
1 Boston Consulting Group (2019)
2 Internet Retailer, BlueSnap, Kount (2019)
3 Ponemon Institute (2019)
4 Visa (2019)
5 Juniper Research (2016)
6 LexisNexis (2019)
7 Juniper Research (2019)
8 Financial Crimes Enforcement Network (2018)
9 Clark Howard (2017)
10 Experian (2018)
11 PCI DSS (2018)

About Payrix

Payrix offers the only fully progressive technology platform that gives software companies the path from integrated payments partner to payment facilitation.

Payrix Launch enables companies early on their journey to quickly and easily start realizing the potential of payment monetization, with no risk, regulatory burden or technology investment.

Payrix Pro is our hybrid solution that provides a payment facilitation-like experience without you holding the risk. Whether you're looking to grow beyond Launch, or working toward payment facilitation but wanting to monetize payments more immediately, this model provides a sweet spot between revenue and risk.

Payrix Enterprise is our full-fledged payment facilitator solution, with a best-in-class tech stack where you fully own your brand's payment experience, as well as the risk. Although the technology investment is a little higher, your revenue potential is maximized.

Talk to us to discover what model is the best fit for your software and learn how to transform your payment processing from a cost center to a profit center.