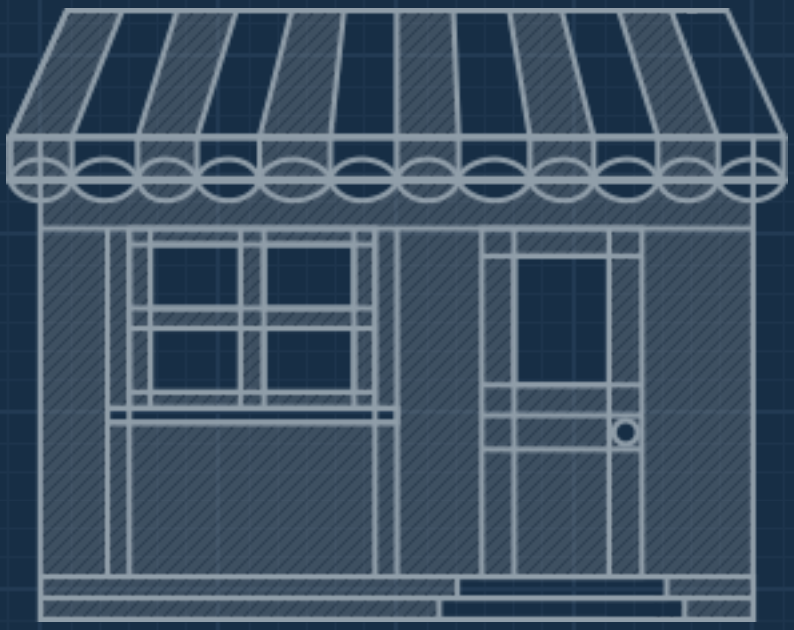
wePAY developer

Platform Payments 101



Your service connects buyers and sellers, and you want to learn more about payments. WePay's Platform Payments 101 will help you discover the realities of facilitating payments on a platform.

Table of Contents

1. Payment Facilitation 2
2. Regulatory Challenges 5
3. Card Network Compliance 11
4. Fraud and Loss 16
5. Minimizing Chargeback Risk 25
6. Technical Complexities 30

Chapter 1

Payment Facilitation

Our main character in the pages to follow is a platform with multiple users looking to let those users accept payments. This hypothetical platform may not have been active for a very long period of time – it may have fewer than a hundred users or so. Nevertheless, this platform has grand ambitions, and is exploring infrastructure options that would allow its users to individually process thousands of dollars, and collectively process tens of millions of dollars.

Flow of funds

When considering how to give its users the power to accept payments, the platform needs to start with one question: at any point should we take ownership of our users' funds? The answer to this question is critical. It locks the platform into one of two potential options.

The first (choosing to take control of user funds) is called aggregation. All funds processed on behalf of the platform's users are collected into one central account under the responsibility of the platform.

The second option involves processing funds directly to the end user. At no point are these funds in an account managed by the platform.

If a platform chooses to aggregate the funds of their customers, they may be defined alternately as a payment facilitator, a payment service provider, a master merchant, or a third party payment aggregator. These terms are pretty interchangeable.

Subsequently, a payment facilitator may be subject to the different regulatory, compliance, and operational challenges that are detailed in following chapters. If the platform decides not to take control of customer funds at any point, they will probably require a payment facilitator to perform this task for them.

The Payments Ecosystem

The online payments ecosystem is composed of the following actors. These terms aren't necessarily industry-standard - other services may describe things differently.

Buyer – The cardholder. This individual gives permission to their (issuing) bank to send money to the merchant/seller's acquiring bank by purchasing a good or service with a credit card.

Merchant/Seller – The intended recipient of a cardholder's money. In the following chapters, they are also an active user of a platform, and accept their payment from the cardholder through the platform.

Platform – A web business that connects customers (buyers) and users (sellers).

Payment Facilitator – An entity that takes legal responsibility for funds in the process of directing them from buyers to sellers.

Payment Gateway – A secure channel that moves data between payment facilitators and higher-level financial institutions like banks or card networks. They provide APIs for a payment facilitator to interact with.

Acquirer – A bank that underwrites the payment facilitator. The acquirer may store funds kept within that payment facilitator's accounts. It also (similar to a payment gateway) connects the payment facilitator to higher-level financial institutions with APIs.

Card Association – A private network that facilitates transactions and settlement between issuing and acquiring banks of the parties involved in a transaction. There are four major card associations in the US: Visa, MasterCard, AmEx and Discover.

Platform Payments 101 is most concerned with the difference between an ordinary platform or marketplace and one which chooses to become a payment facilitator (chooses to take control of customer funds). Platforms should be armed with the information they need in order to treat this choice as an educated decision.

Chapter 2

Regulatory Challenges

Since the signing of The Electronic Fund Transfer Act by President Jimmy Carter in 1978, the rights, liabilities, and responsibilities of consumers who make electronic payments and the companies that offer it as a service have been governed by a complex web of state and federal regulations.

The extent to which any electronic payment is subject to the various statutes regulating financial services depends on the specific nature of the transaction and the risk (financial and otherwise) associated with it. Payment facilitators are doubly subject to regulation, since they sit in the middle of a decoupled transaction. They are subject to one set of regulations when charging customers and another when disbursing funds to merchants. The legal burden is even heavier for companies that facilitate payments to overseas merchants or for regulated goods or services.

Payment facilitators are doubly subject to regulation, since they sit in the middle of a decoupled transaction.

Due to the nature and complexity of the model, payment facilitators often require specialized staff responsible for ensuring regulatory compliance. Outlining the entire regulatory environment and determining which statutes apply to which online platforms is a herculean task; it is certainly outside the scope of this white paper. However, this section covers some of the more potent regulatory issues facing payment facilitators today.

Anti-Money Laundering and Know Your Customer

The Bank Secrecy Act (BSA) of 1970 requires all financial institutions to detect and prevent money laundering. Regulated companies must develop a BSA Anti-Money Laundering (AML) compliance program approved by each company's board of directors.

The BSA has been amended several times over the past four decades, most notably in 2001 with the signing of the USA PATRIOT Act by President Bush. The PATRIOT Act was intended to help government agencies intercept and obstruct terrorism, but it has far-reaching implications for financial institutions and other regulated businesses. To detect and prevent terrorist financing, companies must now verify the identities of individuals using their services to conduct financial transactions. Upon request, these companies must provide information related to potential terrorist activity to the U.S. government.

The PATRIOT ACT also requires businesses to develop Customer Identification Programs (CIP) appropriate to the size and type of their business. A company's CIP outlines its process for obtaining, retaining, and reporting information about its customers. These requirements are often referred to as Know Your Customer (KYC) requirements. KYC processes are employed by companies of all sizes to ensure compliance with the BSA and to prevent identity theft, financial fraud, money laundering, and terrorist financing.

Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) is an agency of the US Department of the Treasury under the auspices of the Under Secretary of the Treasury for Terrorism and Financial Intelligence.

Federal regulations require all companies to comply with OFAC rules, which apply to all financial transactions between any two counterparties.

OFAC provides an updated list of all individuals and businesses (Specially Designed Nationals), with whom U.S. persons and businesses may not do business. To remain compliant, payment facilitators must develop and enforce procedures that ensure their services are not being used by persons on the OFAC list or to support sanctioned activities.

Financial Crimes Enforcement Network

All money services businesses (MSBs) are required to register with the US Department of Treasury through the Financial Crimes Enforcement Network (FinCEN). FinCEN is a bureau of the US Department of the Treasury that collects, analyzes, and coordinates the sharing of information about financial transactions in order to combat financial crimes. Failure to register with FinCen can result in criminal and/or civil penalties.

Once registered with FinCEN, companies are unequivocally subject to the BSA, which - in addition to other obligations - requires companies to file Suspicious Activity Reports (SARs) for activities that might signify money laundering, tax evasion, or other financial crimes.

Companies may also be required to register as Money Services Businesses (MSBs) with the individual states in which they operate. State regulators have

been known to monitor the public FinCEN list for newly-registered companies that have failed to register at the state-level.

Money Transmission

MSBs include companies that provide money transmission services, or the acceptance of "currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."

Virtually all states regulate money transmission through an agency or department located in the consumer affairs or in the financial institutions bureau of the state's executive branch. In most states, unlicensed money transmission can lead to civil and/or criminal sanctions. Individuals that help to operate an unlicensed money transmitting business may be fined and/or imprisoned.

It is not uncommon for a business to take 6 months and spend over $500,000 to obtain state licenses.

While the purpose and content of the state laws may be quite similar, each state has its own unique application and compliance requirements. These requirements can be very expensive in terms of fees, legal costs, and time. States often require lengthy and intrusive background checks and disclosure from senior executives, directors, and investors in order to obtain a Money Transmission License (MTL). It is not uncommon for a business to take 6 months and spend over $500,000 to obtain state licenses. Creating nationwide coverage of MTL licenses can easily take years. In addition, companies are

subject to bonding and net worth requirements which require large deposits of cash or other assets. This can be a prohibitive roadblock for smaller, early-stage companies.

Furthermore, obtaining full licensure involves continuing compliance-related responsibilities and costs, including annual state MTL fees and assessments. There are ongoing reporting, examination (with concomitant annual assessments), bonding, minimum capital, qualified investment, and other compliance requirements from multiple (and in some cases inconsistent) regulators.

Money transmitters must typically create and maintain compliance-related

Determining whether a business is a money transmitter is a matter of locality and circumstances.

support and monitoring functions within the organization to fulfill each state's individual compliance-related requirements. This involves hiring compliance staff and building IT-related infrastructure capable of supporting each state's specific compliance requirements.

Determining whether a business is a money transmitter is a matter of locality and circumstances. Not all platforms that facilitate payments are money transmitters, so platforms are highly motivated to design their payment infrastructure in such a way as to minimize the likelihood of being classified as a money transmitter by state or federal regulators.

Tax Reporting

In 2011, the IRS introduced the Form 1099-K to reduce the discrepancy between the amount of income that people voluntarily report to the IRS and the total amount of income that they should report. The Form 1099-K only reports the movement of funds; individual merchants must decide whether these funds represent taxable income.

The tax code requires payment facilitators to issue a Form 1099-K to every merchant that processes over $20,000 and 200 payments in a calendar year and to file a corresponding form with the IRS. If the company is required to file over 250 forms in a given year, they must file electronically. The Form 1099-K requires the merchant's Tax ID, legal name, address, and total transactions for the calendar year. If the company files inaccurate, incomplete, or tardy returns, it may be fined hundreds of dollars per erroneous filing, with no maximum penalty.

Chapter 3

Card Network Compliance

The Card Associations (e.g. Visa, MasterCard, American Express, and Discover) publish and regularly update their operating regulations and card-acceptance policies and procedures. American Express, for example, updates its two-hundred page Merchant Regulations at least twice a year. All merchants are required to follow these rules in order to accept card payments.

Not only must payment facilitators adhere to the operating regulations, they must force their users to adhere as well. This section outlines a few of the most salient issues that payment facilitators face.

Payment Aggregation

Some platforms, particularly online marketplaces, charge customers on behalf of individual merchants. Amazon, for example, only charges a customer once upon checkout, even though funds are often routed to a diverse group of small sellers. In this scenario, the platform (not the merchant providing the good or service) is the merchant of record. These platforms are considered aggregators.

Aggregation introduces additional risk because the payment facilitator is responsible for accepting and disbursing payments to third-parties, even though it has little control over the quality or delivery of the good or service these third-parties provide.

Aggregators are required to register with the Card Associations, who generally discourage aggregation given the inherent risk of the model. Failure to register is tantamount to “factoring” (the expressly prohibited practice of processing payments for a purpose other than that for which the business was approved). Platforms caught factoring face serious penalties, including the termination of their merchant account, and/or hefty fines.

Platforms caught factoring face serious penalties, including the termination of their merchant account, and/or hefty fines.

Registering as an aggregator requires sponsorship from an acquirer. Acquirers are the banks or financial institutions that accept card payments on behalf of merchants. Not surprisingly, most acquirers are unwilling to underwrite aggregators, given the additional regulatory and financial risk associated with them. Acquirers willing to underwrite these businesses establish approval processes significantly more rigorous than those for less risky business models.

Once approved, aggregators face additional regulations and requirements from the Card Associations. These rules dictate:

- The types of merchants for whom they may process payments.
- The agreement they must execute with each merchant.
- The information they must collect and the checks they must perform for each merchant.
- The merchant information and processing data they must report to the Card Associations.

- The policies and procedures they must develop and submit to the Card Associations for approval.
- The information they must disclose to cardholders and merchants.
- The customer service they (or their sub-merchants) must provide.
- The operating regulations they must enforce.

These additional rules protect the Card Associations from irresponsible aggregators damaging the card network brands.

Payment Card Industry Data Security Standards

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store, or transmit credit card information adequately protect cardholder data. The PCI DSS is administered and managed by the Payment Card Industry Security Standards Council (PCI SSC), a non-governmental regulatory body established by the Card Associations.

While all merchants must be PCI DSS compliant, payment facilitators undergo additional scrutiny. Any platform that stores, processes, or transmits cardholder data for any third party must register with the Card Associations as a Level 1 PCI DSS-Compliant Service Provider, which requires an annual independent security audit and regular network vulnerability scans by an Approved Scanning Vendor (ASV), amongst other equally stringent requirements.

It is not uncommon for a business to take 6 months and spend over $500,000 to obtain state licenses.

Payment facilitators must also ensure the compliance of individual merchants operating on their platforms. These merchants are not exempt from PCI compliance, even if their payments are administered by a payment facilitator; though it may reduce the risk of exposure and thus the effort required to validate compliance.

Failure to comply with the PCI DSS may result in fines, higher transaction fees, and/or termination of the relationship between the Card Associations and delinquent payment facilitator or merchant. Furthermore, platforms that suspect or confirm the unauthorized access, use, theft, or misappropriation of cardholder information incur additional obligations, including the responsibility to notify the relevant authorities and conduct a thorough forensic investigation, potentially by a reputable third-party forensic investigator. The vast majority of individual states have also passed laws that require companies to report data breaches to the affected parties.

Convenience fees

The Card Associations have developed strict rules for how and when merchants can charge transaction fees, which are often an important source of revenue for platforms that facilitate payments between merchants and their customers.

The Card Associations prohibit merchants from prioritizing one payment method over another or applying “surcharges” that dissuade cardholders from using a payment card. They do, however, permit merchants and payment facilitators to

charge convenience fees for the privilege of paying for a product or service using an alternative payment channel.

Unfortunately, the policies that determine what constitutes a compliant "convenience fee" vary by Card Association (and also by applicable state laws). According to Visa, certain criteria must be met in order for a merchant to charge a convenience fee. For example, the fee must be disclosed prior to payment, presented as a flat fee (i.e. not a percentage of the sale), and applied to all means of payment accepted in that channel.

Brand Rules

The Card Associations establish rules, which payment facilitators must enforce, that restrict merchants from engaging in activities that harm or degrade the card network brands.

Determining whether a merchant has followed the official guidelines for displaying an Association logo is fairly straightforward, but ensuring that merchants do not engage in illegal activity, fraudulent, deceptive, or unfair business practices, or the sale of goods or services prohibited by the Associations (e.g. adult digital content, loans, or gambling services) can be quite difficult.

Payment facilitators must also ensure that individual merchants establish policies (returns, refunds, customer service, disclosures, etc.) in accordance with the operating regulations and that they convey these policies to cardholders.

Chapter 4

Fraud and Loss

Most fraud prevention features are designed for card-present environments. Visa, for example, has deployed a number of anti-fraud measures designed to make card reproduction extremely difficult, including holograms and embossed security characters on the face of the card. Moreover, the signature and magnetic strip on the back of the card are designed to ensure that the person using the card is the actual cardholder. Merchants are not liable for fraud when card-present transactions are properly authenticated.

Online platforms, however, typically facilitate card-not-present transactions (card payments made without physically swiping a card). On a website, buyers enter credit card data into a form – they do not hand their card to a cashier. Unfortunately, card-not-present transactions are highly susceptible to fraud and abuse, for which merchants and payment facilitators are held liable.

Chargebacks

When a cardholder disputes a charge with their bank (the “issuing bank”), the bank reverses the payment and refunds the cardholder. This is called a chargeback.

Cardholders are protected from the financial liability of unauthorized credit card transactions by Regulation Z of the Truth in Lending Act and unauthorized debit card transactions by Regulation E of the Electronic Fund Transfer Act. Card Associations have even broader rules with further added protections. When

fraudulent transactions do occur, a well-defined chain of liability determines who is ultimately responsible for making restitution to the cardholder.

Payment facilitators must recover chargebacks from merchants who generate them, or else write off the full amount of the chargeback as a loss.

For chargebacks resulting from card-not-present transactions, the issuing bank recovers the funds from the merchant's bank (the acquiring bank), and the acquiring bank recovers the funds from the merchant.

Since most chargebacks are received weeks or months after the original payment, it is sometimes difficult to recover the funds from the merchant. This is why acquirers are so conservative in their underwriting: an acquirer will typically research the financial stability, creditworthiness, and underlying riskiness of a business; it will implement special funding policies (such as reserves or holdbacks) to mitigate loss; and it will require personal guarantees from business owners, whom it will hold personally liable for the business's financial obligations.

Revenue accrues as tiny percentages of transactions, while losses occur as whole transactions.

Depending on the specific contract it has signed with its acquiring bank, a payment facilitator (not its sub-merchants) may be held responsible for chargebacks. The payment facilitator, therefore, assumes responsibility for recovering funds from the end-merchants and liability for funds that cannot be recovered.

In other words, payment facilitators must recover chargebacks from merchants who generate them, or else write off the full amount of the chargeback as a loss. This is perhaps the most important fact of life for a payment facilitator: revenue accrues as tiny percentages of transactions, while losses occur as whole transactions.

The distaste for aggregation amongst acquirers is not surprising given that the risk assumed by payment facilitators is equal to the aggregate risk of its entire network of sub-merchants. The acquirer must trust the facilitator's policies, processes, and procedures for determining and mitigating loss since it has no insight into the risk profiles of individual sub-merchants.

Payment facilitators also interact with both merchants and their customers, so they must understand the risk associated with both. The four categories of risk include:

Merchant Identity Fraud

In this scenario, a fraudster establishes a merchant account on behalf of a seemingly legitimate business, charges a number of stolen credit cards, and disappears with the proceeds before the cardholders discover and reverse the unauthorized transactions. When the payment facilitator attempts to recover the funds, the fraudster is long gone, and the payment facilitator is liable for both the loss and any additional fees or assessments associated with the chargebacks.

This happens more often than you may think. Just recently, the Federal Trade Commission uncovered a four year operation in which fraudsters established more than one-hundred merchant accounts (using the Employer Identification

Numbers of real businesses) to bilk cardholders and acquirers of more than $10 million.

Everyday, fraudsters are getting better at obtaining the information necessary to assume false identities (e.g. birth certificates, government-issued IDs, credit reports). It is impossible to definitively verify the identity of an online merchant, since any information that legitimate users present to prove their identities can be obtained by an imposter. The true identity of an online merchant simply cannot be ascertained with total certainty.

In some cases, fraudsters use “money mules” to obfuscate their illicit activities. A typical scam involves the fraudster charging stolen credit cards and settling the proceeds to a mule. The mule keeps a percentage of the money and transfers the remainder to the scam operator, typically located in another country. Mules are often unaware that these funds are the product of illicit activity. They are usually hapless victims duped by get-rich-quick schemes or promises of legitimate employment. Unfortunately, they are complicit in the scheme, and they risk both criminal and financial penalties. When cardholders dispute the unauthorized transactions, the payment facilitator attempts to recover the funds from the mules bank account. In most cases, however, the mule has already transferred the funds to the scam operator.

It is impossible to definitively verify the identity of an online merchant, since any information that legitimate users present to prove their identities can be obtained by an imposter.

Merchant Credit Risk

In this scenario, a legitimate merchant defaults on its obligation to fund chargebacks. Although payment facilitators do not issue loans, they do take credit risk by settling funds within the chargeback window. The chargeback window varies by card type, but it is usually at least 90 days, and payment facilitators are ultimately liable for all payments settled to merchants within that range.

Merchant credit risk is greatest among younger, less-established, or riskier businesses. Not surprisingly, these businesses often use payment facilitators explicitly because traditional acquirers are unwilling to take their business. Unfortunately, the hesitation to underwrite these businesses is not entirely unjustified, given the higher likelihood of excessive chargebacks and bankruptcy.

A website that connects homeowners with local service providers, for example, has no control over the quality or delivery of the services provided. The platform simply cannot guarantee that the service will be delivered on time and as advertised. If, for whatever reason, the service is unacceptable and the homeowner decides to charge back the payment, the facilitator must recover the payment from the merchant or eat the cost itself.

Traditional acquirers mitigate this risk by analyzing a merchant's processing and/or credit history, but that involves a longer underwriting process and assumes that merchants have a pre-existing processing history or credit score.

Crowdfunding platforms that allow entrepreneurs to take pre-orders are particularly susceptible to credit risk. If the entrepreneur fails to deliver the product on time or as advertised (e.g. manufacturing is more expensive or time

consuming than anticipated, etc.), customers will likely charge back their payments.

The payment facilitator is liable for these chargebacks if they cannot recover the funds from the entrepreneur. Even though the payment facilitator is not issuing entrepreneurs a loan, per se, it is incurring risk based on the creditworthiness of that entrepreneur or his business (presumably not that great, given the fact that most companies raising money on crowdfunding platforms are startups).

Crowdfunding platforms that allow entrepreneurs to take pre-orders are particularly susceptible to credit risk.

In July 2012, Pebble Technology raised $10.27 on Kickstarter to develop and manufacturing its signature smartwatch. Fortunately, Pebble successfully manufactured the product and fulfilled the orders, but had they not, Pebble would have received a flood of chargebacks from customers that never received their orders. And if Pebble could not make good on these chargebacks, the payment processor (Amazon in this case), would have been liable for over $10 million.

Processors generally frown on young companies that accept pre-orders or deposits long before they fulfill orders because the greater the amount of time between payment and fulfillment, the greater the risk that merchants fail to deliver and the larger the financial liability. It is therefore not surprising that some payment processors are simply unwilling to support the use-case.

Buyer Identity Fraud

In this scenario, a fraudulent customer uses a stolen credit card (or a card established with a stolen identity) to purchase a product from a legitimate merchant. By the time the real cardholder discovers the fraudulent charges, the fraudster already has possession of the goods.

While cardholders may not be liable for unauthorized transactions, merchants have no such protection. When the real cardholder inevitably reverses the payment, the merchant is out the cost of fulfilling the order, the revenue of the sale, and the fees associated with receiving the chargeback.

While cardholders may not be liable for unauthorized transaction, merchants have no such protection.

Payment facilitators must address merchant credit risk in this scenario, since legitimate merchants may be unwilling or unable to refund payments for valuable goods or services that have already been delivered.

Furthermore, merchants selling goods or services through online platforms typically expect the platforms to protect them from fraudulent buyers - especially platforms that play an active role in connecting buyers and sellers. Take an auction site for example: a legitimate merchant lists a valuable collectible on the site, promptly ships the item to the highest bidder, and never receives payment because the buyer was a fraud.

Although platforms can hold merchants responsible for chargebacks resulting from buyer fraud, it may not be worth it. Most online marketplaces are highly motivated to protect the quality of their networks: the moment merchants doubt the integrity of a marketplace, they will look for a safer venue in which to conduct business.

These buyer-fraudsters can be very savvy in the techniques they use to prey on merchants. Imagine a scenario where a legitimate seller is trying to rent out his apartment on Craigslist. Out of the blue, somebody calls him and says that they'll send him the rental money via a payment facilitator like WePay. The seller sets up a WePay account, and receives "the buyer's" credit card number for one month's rent. The renter then "accidentally" overpays the seller or decides that they don't want to live in the apartment anymore. They ask the seller to refund them by sending a check or wiring the money (or by any other means other than refunding the credit card). The seller sends them the refund, and a few weeks later the real cardholder disputes his fraudulent charge. WePay is forced to target the innocent apartment owner (who unknowingly charged the stolen card).

Friendly Fraud

Friendly fraud is similar to buyer identity fraud save for a few important differences. In both cases, the merchant is the victim of a fraudulent buyer, but with friendly fraud, the buyer is actually the cardholder. The cardholder duly authorizes the payment, but reverses it once they have received the product or service. The cardholder gets the goods for free, and the merchant gets stuck holding the bag.

Friendly fraud is nearly impossible to detect because the payments themselves are actually legitimate. Worse still, merchants accepting card-not-present payments really have no way to prove that cardholders authorized the payments, since they never swipe a physical card or receive a signature from the cardholders.

The protections afforded to cardholders may play a role in promoting friendly fraud. Since there is such a low barrier to disputing “unauthorized” card-not-present transactions, cardholders can sometimes simply charge back a purchase to avoid paying for it.

Like buyer identity fraud, the cost of friendly fraud is even greater than the purchase price, since merchants also invest time and effort into finding the customer, fulfilling the order, and fighting the chargeback. In fact, LexisNexis reports that on average chargebacks cost merchants 2.33 times the amount of the original purchase. The additional cost includes interest/fees paid to financial institutions and replacing/redistributing merchandise.

Chapter 5

Minimizing Chargeback Risk

For a payment facilitator, preventing losses is equivalent to preventing chargebacks. This may seem like a relatively simple goal: reduce chargebacks to an absolute minimum. Unfortunately, the means to achieving this goal is incredibly complex.

As discussed in Chapter 4, many scenarios can result in chargebacks. The process of preventing chargebacks is not as simple as detecting the use of stolen credit card numbers. Each type of fraudulent or risky behavior necessitates its own set of protections. This means that for a payment facilitator, loss prevention is an inherently complex process.

Detecting Merchant ID Fraud

In order to prevent fraudsters from impersonating actual merchants, a payment facilitator has to have a good system for verifying a user's identity. To verify identity in real-time (an important feature for most major platforms), a facilitator must collect and analyze massive amounts of data. This often involves the use of third-party technologies to validate a user's provided credentials. With so much overlapping data, identity verification is rarely a Boolean operation. Payment facilitators are more often faced with users that fall somewhere along a spectrum between verified and unverified.

Identity verification is rarely a Boolean operation. Payment facilitators are more often faced with users that fall somewhere along a spectrum between verified and unverified.

Once identity has been assigned a given probability, payment facilitators may still face problems with false positives (a valid merchant marked as fraudulent) and false negatives (a truly fraudulent merchant that is allowed to process transactions). PayPal has been widely criticized for their decisions to freeze accounts when they've assumed false positives.

Because of their exposure to chargebacks, if a payment facilitator makes a false negative and allows a fraudulent merchant to process transactions, they risk having to write off all of those transactions as losses. Even more distressingly, fraudulent behavior is rarely limited to one merchant. Fraudulent users often test a system's weaknesses by working together in large, anonymous fraud rings across multiple accounts. If these fraudsters are successful, a payment facilitator will lose large amounts of money very quickly.

Unfortunately, any safeguards put in place to slow down fraudulent or risky activity will also get in the way of good merchants that want to receive their money as quickly as possible. There is a natural tradeoff between providing an enjoyable user experience and building protections against fraud. Traditional merchant accounts involve multi-page applications, credit checks, and waiting periods before a merchant is allowed to accept payments. Because they are required to maintain a good user experience, payment facilitators can rarely use those same protections.

Assessing Merchant Credit Risk

Though verifying identity is a challenge, it's actually much harder to identify merchants who, while not exactly fraudulent, pose risk to the platform by the simple act of failing to deliver their products or services on time or as advertised to their customers. Unless you're running credit checks, verifying a bank account balance, reviewing prior processing history, reviewing business policies, or auditing financials, you have very little insight into the credit risk of the business. Platforms can combat this by limiting the amount of funds an individual merchant can process or withdraw, but this obviously decreases the quality of the merchant's experience.

In both cases (identity fraud and merchant credit risk), payment facilitators may require merchants to post collateral ("a reserve") to ensure that they can cover any chargebacks they receive (this reduces the exposure of the payment facilitator).

The reserve requirement for a particular merchant is determined by the payment facilitator and its assessment of the merchant's risk. Facilitators can also hold a percentage of a merchant's payments or delay settlement for days, weeks, or months to minimize credit risk. Payment facilitators should establish reserve requirements proportional to their own risk level and develop procedures for updating and communicating those requirements to merchants whenever appropriate.

However, even the most sophisticated techniques in the world cannot abolish risk and fraud completely. Therefore, processors have to establish policies and procedures for recovering funds from merchants, referring them to internal or third-party collections, or pursuing legal recourse when necessary.

Managing Disputes

Not only should payment facilitators implement sufficient safeguards to prevent fraud and recognize suspicious activity, they must also implement processes to manage and resolve disputes between buyers and sellers.

As the merchant of record, payment facilitators receive chargeback notifications from acquirers and must reconcile the chargeback to its original transaction. In addition to recovering funds from merchants, payment facilitators are also responsible for notifying merchants and providing a means by which merchants can defend themselves against chargebacks.

There are hundreds of chargeback reason codes and they differ by each card network, so understanding the root cause of a chargeback may not be easy.

The documentation needed to successfully represent a chargeback depends on the chargeback reason code. There are hundreds of chargeback reason codes and they differ by each card network, so understanding the root cause of a chargeback may not be easy. Furthermore, the documentation required to fight a chargeback is often split between the merchant, who fulfills the order, and the payment facilitator, who authenticates and verifies the cardholder.

Some payment facilitators have productized the dispute-resolution process to preempt formal chargebacks. In this scenario, buyers dispute payments through the payment facilitator before filing a complaint with their issuing bank. The payment facilitator then attempts to resolve the dispute between the buyer and seller directly without involving the issuing bank or the acquirer. There is

significant operational overhead associated with this method, but it can dramatically reduce chargebacks, especially in cases of “accidental” friendly-fraud (i.e. the cardholder authorized the payment but does not remember or recognize the charge when it appears on their statement).

Chapter 6

Technical Complexities

Even before a platform or a payment facilitator has to worry about fraud, they have to figure out how to process payments from a technical perspective.

For developers, the act of processing payments has been relatively simple for quite some time. Payment-specific APIs have existed since before the advent of PayPal, though they've grown in sophistication and reliability over the past 15 years. Processing thousands of payments into one single merchant account isn't very complicated. For a payment facilitator, it is routing thousands of payments to a variety of merchant accounts that introduces the real challenge.

Coding the Payments Stack

Ideally, a payments facilitator would only have to interact with one API: that of their payment gateway. Gateways exist specifically to reduce the number of technical endpoints that a processor is required to interact with. Instead of making API calls to every card-issuing bank, card association and ACH network, a payment facilitator can simply communicate with a gateway that will take responsibility for routing information to the appropriate institutions.

If a payment facilitator is interested in processing payments directly to their end merchants, a payment gateway's basic offerings may not be sufficient.

Almost all payment gateways, however, are optimized to process credit cards into

a single account. If a payment facilitator is interested in processing payments directly to their end merchants, a payment gateway's basic offerings may not be sufficient. Here, the payment facilitator may have to make sure that these merchants can be uniquely identified within a higher-level financial network, which may involve registering (boarding) them with an acquiring bank. This would probably require integration with another API.

A good integration with these two APIs (payment gateway and acquiring bank) should allow a platform to process transactions and onboard merchants effectively. The question still remains, though – how should these transactions be redirected to the merchants themselves? For this problem, the platform will need to interact with a third API for merchant settlement.

When a merchant/user requests their money be withdrawn to their own bank account, the platform will need to send instructions to the bank where that merchant's money is being held. This 'on-behalf-of' bank is not always the same thing as the acquiring bank. A payment facilitator may aggregate its merchants' money in an account at a separate institution – this is an operational decision. Regardless, in order to withdraw on behalf of a merchant, the platform will need to send instructions to their aggregating bank and monitor the status of the withdrawal.

Accounting and Reconciliation Requirements

These overlapping API integrations present a huge back-office/accounting challenge to the payment facilitator. The key problem is one of reconciliation: at any given point of time, how do debits and credits balance out?

Even though a payment facilitator ‘only’ has to interact with a few APIs, money is arriving into its accounts from a variety of financial institutions. American Express, for example, operates its own network. When a platform charges an AmEx card, AmEx sends the money directly to that platform’s account via the AmEx network. Other card networks may settle their transactions through the payment facilitator’s acquiring bank. ACH payments may arrive through yet another channel.

Payments that arrive in a payment facilitator's account will probably belong to a various merchants. Small pieces of the payments, however, may belong to parties that assisted in facilitating the transaction. Card networks, acquiring

The key problem is one of reconciliation: at any given point in time, how do debits and credits balance out?

banks and payment facilitators themselves all take a small slice of transactions. This practice is central to their business model. Standardizing how these small slices are taken is a huge headache for the facilitator. Should the card network ‘net-out’ their fees before the transactions arrive? Or should they charge the facilitator on a monthly basis?

When making this decision, a payment facilitator has to consider how they will eventually calculate their overall costs. This task is complicated by the fact that card networks and acquiring banks extract wildly different costs per payment. If a customer makes a purchase with a rewards credit card, for example, that per-payment cost will be much higher then if they make the same purchase with a simple debit card. The payment facilitator must keep track of these per payment differences in fees, and they must make sure the fees are withdrawn from the correct segment of their funds – funds that are by definition constantly being facilitated from payers to recipients.

Chargebacks once again make life difficult. As chargebacks and refunds are forcibly withdrawn from a payment facilitator's accounts, the facilitator must choose how to fund those charges. In the process of fighting the chargeback, at what point should it be considered a loss and written-off? How can this loss be tracked effectively in order to better combat it? At a certain level, these fundamental questions become accounting problems as well.

Timing and Payment Failures

Because a payment facilitator takes responsibility for so much of the payments stack – the technology layers separating buyers and sellers – errors can arise from all kinds of interactions outside of their control. Payments can fail in dozens if not hundreds of different ways, including after a system has indicated one has succeeded.

Traditional gateways do little, if anything, to insulate a facilitator from this complexity. As a result, developing against a payment gateway means that much of a payment facilitator's code exists to handle different error scenarios, rather than actually process payments. Building appropriate fail-safes takes much iteration to get right, and constant monitoring to ensure nothing new has come up.

Even the simplest credit card transaction involves three sets of API interactions: authorization, capture, and settlement. Authorization and capture are often built to fire simultaneously, but if a payment facilitator wants to analyze the transaction with its own proprietary risk systems, authorization/capture can be separated by a period of time. This means individual transactions are exposed to failures at three separate times during their life cycle.

Since the payment facilitator and/or platform assumes responsibility for communicating these failures to the user, it becomes a huge exercise in user experience design to do so effectively.

Transactions are exposed to failures at three separate times during their life cycle.

This challenge is compounded by additional questions – how much of the failure does the customer need to understand, and how much information would assist a malicious user? After all, fraudsters stand to gain from any piece of information that helps them design more effective attacks.

Ordinary Worries, Higher Stakes

Payment facilitators also have to worry about the same technological challenges that plague most internet companies: data integrity and connectivity in particular. When dealing with payments, however, the consequences of failures are always financial losses. These possibilities require the most stringent preventative measures.

Data integrity is particularly crucial to a payments facilitator because so many of its core functionalities (payment processing, merchant onboarding, etc.) involve reliance upon external APIs. This creates a data layering issue – a facilitator must track processes in both its proprietary data and also in data generated by its partners.

When settling funds to merchants, for example, a facilitator must record a withdrawal request within its own databases. Whether that request is ultimately successful can only be determined by the facilitator's partner bank, and this

request may take days to process. If it ultimately fails, this too must be recorded and communicated.

For a single merchant's withdrawal, three pieces of information might exist in the payment facilitator's database (initial withdrawal request, initial withdrawal

Reconciling proprietary data with externally generated data is a constant headache.

authorization, eventual withdrawal failure). When looking at the partner bank's records, however, this line item may only appear once (withdrawal attempt – failed), or it may never appear at all. Reconciling proprietary data with externally generated data is a constant headache.

As any developer knows, networked computers very frequently have connectivity issues. Most modern browsers and applications do a good job hiding this, but API integrations are low-level communication that don't get such friendly abstraction layers. While no software solution can prevent these connectivity issues, many older payment gateways only magnify problems of idempotence (the idea that a function, or API call in this case, can be fired many times with only one eventual result). Idempotence is a hugely important concept in online payment APIs because multiple, unintentional charges can destroy a payment company's reputation.

Idempotence is a hugely important concept in online payment APIs because multiple, unintentional charges can destroy a payment company's reputation.

When connectivity issues make it difficult to see if a charge or withdrawal has gone through, it's up to the payment facilitator

to make a judgment call. These situations can be even more tricky than communicating a high-level error message to a user, because the problem is really the absence of information. Fail-safes and protections against these problems are a hugely important piece of any payment facilitator's payment processing code.

Some modern payment gateways embrace new developments in hiding these problems, and are better about, for example, not charging a card a second time when re-submitting after a network error left the originating system unsure of whether the payment was authorized.