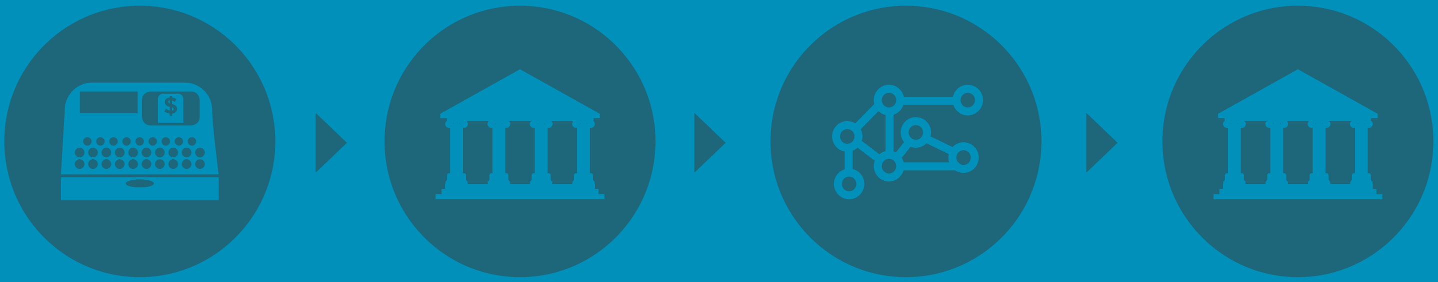
2CHECKOUT



How Credit Card Processing Works
The Payments System Simplified

How Credit Card Processing Works
The Payments System Simplified

Author : : Thomas Kossler

This is the second of a two white papers focusing on the growth of payment systems and the life of a transaction. In this section we will discuss the flow of transactions and other payment system considerations important to all merchants, but especially e-commerce merchants.

Table of Contents

The Basics

With the last white paper, **The Evolution of the Payment System**, defining the players and market dynamics that drove the growth of online payments, this white paper focuses on the movement of payment system transactions in retail and e-commerce. The common credit transaction provides the basis of this exploration, which consists of a two-step process: authorization and clearing. This is different from a one-step transaction, such as that of an ATM machine transaction.

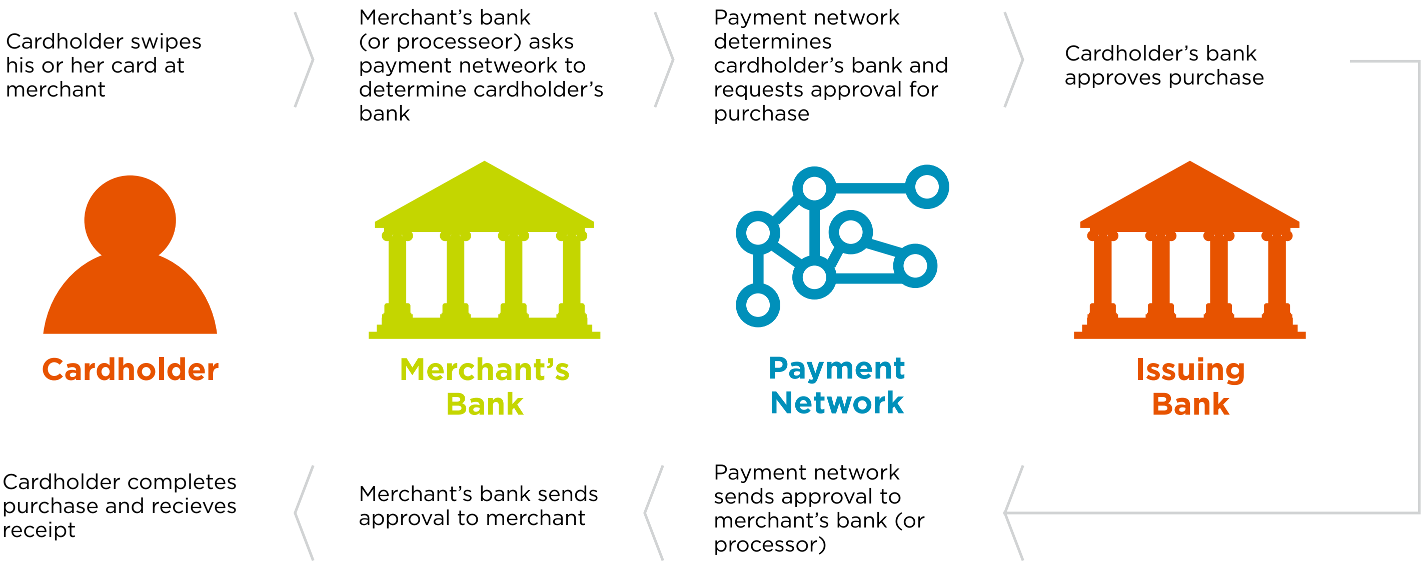
In the first step of this process, an issuing bank accepts an applicant for a new account with a credit or debit card. The new cardholder is assigned a line of credit and issued a plastic card embossed with the account number, new cardholder's name, and the expiration date of the card. On the reverse side of the card lies a magnetic stripe encoded with the cardholder's name and account number. The back of the card has a spot for the cardholder's signature and — more recently — a 3-digit card verification value (CVV) unique to the card, used for proving its presence and combatting fraud.

The cardholder presents the card to the merchant for a purchase, or more commonly today, swipes his or her own card on the merchant's point-of-sale (POS) terminal, such as a self service kiosk at a grocery store. Through various mechanisms (phone line, data link, internet), the POS terminal sends an authorization request to the merchant's bank, or more typically, the bank's processor. The bank or processor determines which network should receive the authorization and, either through a direct link or via a gateway provider, the authorization request arrives at the association's network center. By reading the first six digits of the card number, the network center determines which issuer — or issuer processor — should receive the request. Upon receiving the request, the issuing bank (or its processor) determines if the account/card is valid, and whether the amount of the request is within the cardholder's line of credit. The response to the request — approved or declined — is returned through the same path back to the merchant's POS terminal, and the sale concludes.

The cardholder is provided with a receipt, and may or may not need to sign the merchant's copy of the sales draft, depending upon the type and amount of the sale. The data representing the sale is stored in the POS terminal's memory.

Generally at the close of business, the merchant "batches out" his or her terminal by sending the sum of the day's transactions, and its accompanying details, to his or her acquiring bank or the bank's processor. The bank or the processor consolidates these sales batches with those of its other merchants and transmits this purchase information to the bank association's network center. This process is sometimes referred to as introducing the sales into interchange, or submitting "clearing" transactions.

Authorization (At Time Of Purchase)



Cardholder swipes his or her card at merchant

Merchant's bank (or processeor) asks payment netweork to determine cardholder's bank

Payment network determines cardholder's bank and requests approval for purchase

Cardholder's bank approves purchase

Payment network sends approval to merchant's bank (or processor)

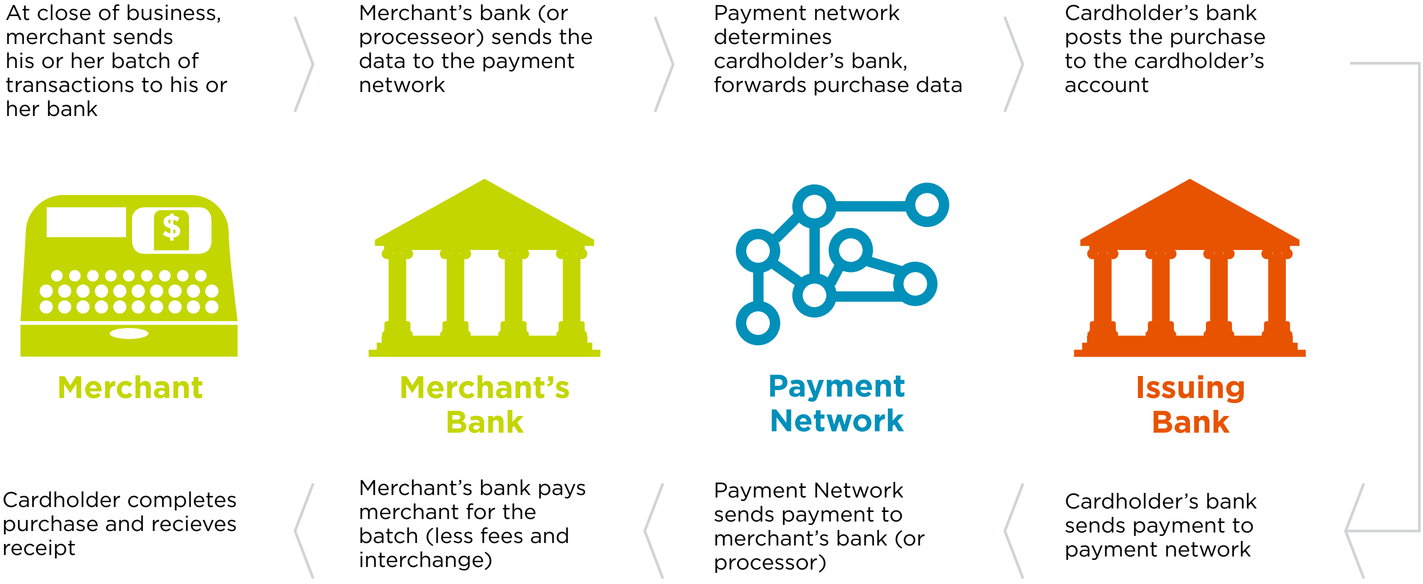
Merchant's bank sends approval to merchant

Cardholder completes purchase and recieves receipt

The bankcard network center reconciles the data from the acquirer and determines the amount due to the acquirer, less interchange, assessments, and other fees. The bankcard network center takes the data received from hundreds of acquirers, reorganizes it by issuing bank, and sends the purchase information to the cardholder's bank where it is posted to his or her account. While not important to merchants, the issuing bank posts statements to the cardholder for the transactions and accepts and applies payments to the account on a schedule agreed to with the cardholder.

Usually within one or two business days, the cardholder's bank sends payment for the transactions (less interchange) to the bankcard network center, which in turn routes funds to the acquirer. At a schedule agreed to between the acquirer and the merchant, the acquirer deposits the funds for the batch into the merchant's bank account. The amount deposited is net of interchange, assessment fees, the acquirer's margin, and other fees agreed to between the acquirer and the merchant. This process is known as "settlement."

Clearing/Settlement



At close of business, merchant sends his or her batch of transactions to his or her bank

Merchant's bank (or processeor) sends the data to the payment network

Payment network determines cardholder's bank, forwards purchase data

Cardholder's bank posts the purchase to the cardholder's account

Cardholder's bank sends payment to payment network

Payment Network sends payment to merchant's bank (or processor)

Merchant's bank pays merchant for the batch (less fees and interchange)

Cardholder completes purchase and recieves receipt

This process doesn't always unfold as planned. Cardholders sometimes return merchandise for a refund, or there is some other purchase-related issue for which a credit adjustment is necessary. The payment system does not authorize returns or credit adjustments. The transactions are created on the POS terminal, receive the proper management authorization or code, and are captured in the day's batch of transactions. At the close of business, the refund or adjustment is included with sale transactions. Sale and return transactions have different transaction codes to distinguish them within a batch. The data is introduced into interchange by the merchant's acquirer, and ultimately reach the cardholder's issuing bank where the credit is posted.

Some problems may occur after a sale is completed that result in transaction retrievals and chargebacks. A cardholder with his or her bank frequently initiates retrievals when he or she does not recognize a purchase on his or her monthly card statement. There are certain data standards on the presence and length of the merchant name associated with a transaction. But the name shown on a statement isn't always the name the cardholder associates with the purchase. In such cases, the issuing bank initiates a retrieval request with the payment network. In some cases the merchant's acquirer has additional information that might resolve the question, but more often than not, the request is sent to the merchant to provide additional purchase details, such as the name of the purchaser, the items purchased, where the goods may have been delivered, etc. In modern families where credit accounts might be shared among spouses and adult children, this additional information may be enough to resolve the inquiry. If not, the retrieval could result in a chargeback.

Chargebacks represent a reversal of a purchase; that is, the purchase is "charged back" to the merchant. The reasons can be many and often include a deliberate or inadvertent violation of the card acceptance rules of the merchant. For example, a merchant may fail to properly authorize a purchase made with a stolen card. Another common reason for a chargeback is that the purchase was unauthorized by the cardholder. This can sometimes comprise a gray area, especially in disputes where a family member uses a parent or spouse's card without his or her permission. Other times the goods ordered are not delivered, or were delivered but not signed for, and the cardholder does not receive the goods. A difficult situation for merchants occurs when the cardholder asserts that the merchandise or service was not as described.

For most disputes, the payment system strongly encourages the cardholder and the merchant to directly communicate about and hopefully resolve the issue. The cardholder and merchant are the two parties present at the purchase who best know what took place. This meeting is also an opportunity for a merchant to save what may be a repeat customer by making a modest adjustment. But when a resolution cannot be reached, the issuing bank initiates an electronic dispute or chargeback with the payment system. Upon receipt, the acquirer forwards the dispute to the merchant for response. If a resolution cannot be reached in the allotted time, the merchant's bank account is debited for the amount of the purchase. In cases where the chargeback results from improper actions by a merchant, the chargeback is processed immediately and the funds are taken from the merchant's bank account.

Payment system participants take chargebacks very seriously. There are extensive rules and regulations pertaining to chargebacks that acquirers and merchants must follow. Programs rapidly identify merchants that do not properly process sales or respond to disputes. Time frames for merchant responses are often very tight. A quick and complete response to a dispute is the only way to ensure a merchant's perspective is heard. That said, this is an appropriate time to look a little more closely at the rules of payment systems.

RULES OF THE ROAD ▶

Rules Of The Road

A few key documents define the legal basis of how a merchant accepts cards. First, each merchant (or sub-merchant, discussed later), signs a card acceptance agreement with his or her acquiring bank. Typically, these forms are three-party agreements that also include the acquiring bank's processor.

The agreement authorizes the merchant to accept cards for that payment system: it outlines the general obligations to follow the rules of the payment system and typically authorizes the acquiring bank, or its processor, to immediately terminate the agreement for cause. This speaks to the arrangements for the payment of settlement, and it specifies the fees the merchant will pay for transactions. One common theme in all merchant agreements is that the merchant must be familiar with, and closely follow, the rules of the payment system. These rules are called "Operating Regulations."

When you consider that payment systems must operate across geographies, cultures, and languages with hundreds of thousands — if not millions — of participants, it becomes apparent why the actions of all system participants must be closely regulated. And they are.

The Visa system's International Operating Regulations (most recently dates 15 April 2013 as of publication) consists of 1,257 pages. Similarly, MasterCard's regulations (issued in three parts: general, chargebacks, security) dates 14 June 2013 and numbers 1,183 pages. Both sets of regulations generally speak to issues including: roles of participants; licensing and licensed activities; use of the brand at the point-of-sale and in advertising; rules to be followed by acquirers; rules to be followed by issuers; allowable activities of service providers and who bears responsibility for their actions; transaction and processing flows; data requirements; security; disputes; and unique geographical requirements. Experienced merchants know that it is important for them and their back-office staff to fully understand the requirements of their acquirer and the payment system.

THE RISE OF THE INTERNET ▶

The Rise Of The Internet

The rapid and pervasive growth of the internet has brought tremendous opportunities and challenges to traditional payment systems.

Obviously, the reach of the internet has opened up wonderful opportunities for cardholders to purchase goods securely from around the world. Similarly, merchants — once restricted to customers who were within living or traveling distances of their locations — can now offer their goods and services globally. E-commerce has grown rapidly, and at the time of this writing fully represents 5% of the total retail volume in the United States. But it wasn't always a sure thing that e-commerce would grow as rapidly as it has.

In the early days of the Internet, consumers weren't sure about the security of their credit card information when making purchases online. A number of specialty applications and products were developed to scramble card numbers and encrypt identifying information. But it was the combination of HTTPS and the PCI standard that enabled consumers to feel comfortable about this new purchasing environment.

Briefly, HTTPS, or Hypertext Transfer Protocol Secure, is a communications protocol for secure communications over a computer network. It provides authentication of the website and server that a user interacts with to guard against "man-in-the-middle" attacks, and it provides bidirectional encryption of the data between endpoints. This guards against eavesdropping or tampering with data when communicating. HTTPS provides a reasonable guarantee that a user is communicating with the website he or she intended to communicate with, and that the contents of the communication cannot be read by outside parties. Nearly all merchant websites employ HTTPS.

The PCI standard — Payment Card Industry Data Security Standard — was a joint effort by the payment systems to provide rigorous controls around cardholder data to reduce any credit card fraud that might arise from the exposure of this data. In effect, issuers wanted to create an additional level of protection by requiring that merchants meet minimum levels of security when they store, process, and transmit cardholder data. Merchants are required to verify PCI compliance on an annual basis.

PCI standards are very thorough and include requirements such as (not a complete list): maintaining a secure network through firewall configurations; protecting stored cardholder data and encrypting it when it flows across open, public networks; managing vulnerability by maintaining anti-virus software; implementing strong access controls by restricting both physical and programmatic access to cardholder data, and ensuring it is only released on a business need-to-know basis; monitoring the access to cardholder data and regularly testing these security systems and processes; and maintaining an information security policy. Thankfully, merchants can normally look to their acquirer for guidance and resources in complying with PCI standards. But ultimately the requirements — and liability if disregarded — are on the merchant.

The security barriers erected around card information by card programs and payment systems has enabled the confident growth of e-commerce. But the use of the internet for payments had one consequence the payment systems didn't fully anticipate.

PCi Security Standards Council™

One of the strengths of the bankcard payment system business model was that it was both costly and difficult to replicate the global infrastructure of data centers, communications links, and operational facilities. The enormous financial resources required to establish a new payment system gave Visa and MasterCard room to dominate the market for payments over time. But the internet began to erode that advantage.

Once data security issues had been largely resolved, other non-traditional payment systems — notably PayPal — leveraged the infrastructure of the Internet to offer payment products that competed directly with the bankcard associations. The enormous global data infrastructure of banks was no longer a "barrier to entry." The physical network was now relatively easy to duplicate via the internet.

Not only did these developments highlight the increased needs of merchants, but they also pressured issuers to assume the roles of non-card based account solutions, such as wireless phones and chip-based devices. This challenged the ability of issuing banks to maintain the same brand recognition of the payment system and banks.

One final consequence of the growth of e-commerce has been the rise of an entirely new network participant: the Payment Service Provider (PSP) or Payment Facilitator (PF). These new third parties (PSP is the Visa term, PF is used by MasterCard) provide the payment link needed by internet-based retailers to complete an e-commerce sale transaction.

Simply put, the PSP integrates with the merchant's shopping cart, is called upon demand, and forwards the transaction to the appropriate endpoint. But if this basic description presented the full value of the PSP, it wouldn't be nearly as exciting for merchants as it has turned out to be. In creating the PSP/PF concept, the bankcard payment systems finally reached out to the newer, thriftier entrepreneur.

As previously mentioned, card acceptance for a retailer was created through a merchant services agreement between the merchant and his or her acquiring bank. Banks had fairly conservative standards for merchants, such as length of time in business, level of capital, established credit histories with vendors, and other business viability measures carried over from bank lending. Many smaller, newer firms could not meet those standards and were relegated to accepting cash only. The new PSPs changed this.

PSPs now represent the "merchant" within the bankcard payment system. And when properly certified, they may accept sub-merchants for whom they process. These sub-merchants do not normally have to meet all of the exacting standards needed to be a full merchant. It's the perfect solution for internet startups.

Sub-merchants must still sign an agreement between themselves and the PSP and acquirer (and agree to follow Operating Regulations), but the PSP provides a somewhat nurturing environment as sub-merchants develop. And if the sub-merchants' success leads to higher volumes, they can keep their processing arrangements with their PSP and transition to a full merchant relationship with the acquirer. The PSP system has led to an explosion in the number of "cottage" businesses that can now accept cards for payment over the internet.

With all of these opportunities, how does an Internet retailer choose the best solution? One approach many have found successful is to choose a PSP with a holistic payments solution. What does that mean? Let's take a minute to review some of the key processes any e-commerce merchant needs.

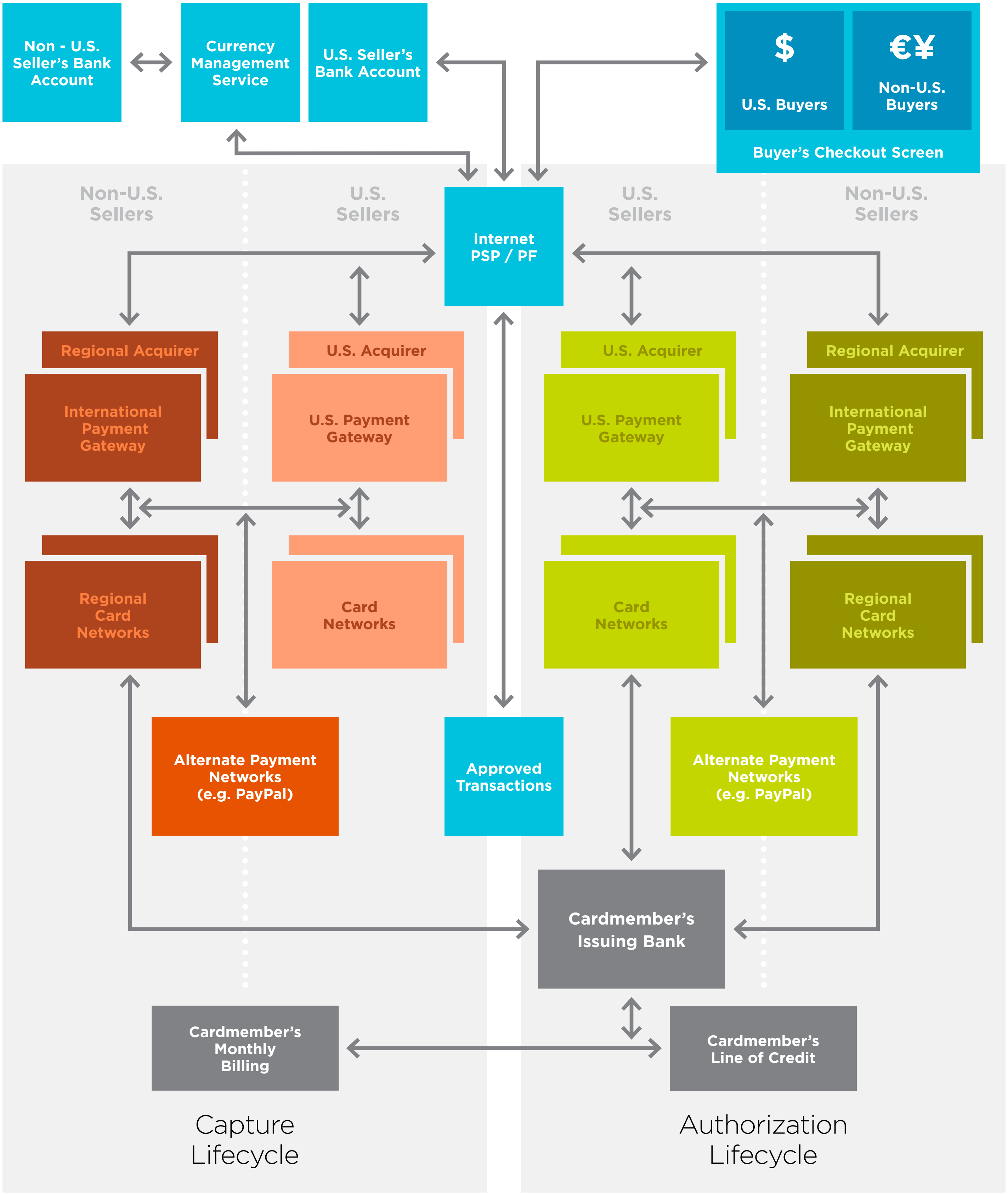
There are six key elements to the e-commerce value chain: portal management, attracting consumers, content management, merchandising, payments, and fulfillment. Some PSPs focus on the narrow definition of payments. Others can bring referral partners and established integrators to a solution that gets the business up and running quickly.

PSPs also offer an expanded breadth of payments in multiple geographical offerings. The established bankcard giants in the United States — Visa and MasterCard — are not necessarily the preferred solution for consumers in other countries. For example, German consumers prefer to pay using Direct Debit ELV and Giropay; French consumers primarily use Carte Bleu; those in the Netherlands prefer iDeal; the Japanese use JCB cards widely; South Koreans use the LG card. And all of these consumers universally prefer to see prices in their local currencies.

If the payments solution provider is U.S.-centric and does not support — or only minimally supports — alternative payments, languages, and currencies, their merchants and sub-merchants will struggle to draw customers from outside their region.

With that said, not all PSPs are authorized to provide payment services in all areas. The major payment systems, Visa and MasterCard, divide the globe into regions: six regions for Visa, five for MasterCard. PSPs must meet stringent business requirements before they are authorized to process and settle transactions within a region. Multi-region PSPs are available, and prospective e-commerce merchants know to choose a solution provider with the broadest possible reach.

Payment Graph



ABOUT ▶

Conclusion

The goal of this white paper is to provide a fundamental overview on payment systems, how they evolved, how they work, and important considerations for digital e-commerce retailers. The bankcard payment systems have been hugely successful over the past fifty years. But there are new challengers, and the needs of merchants are continually evolving. It is, and will continue to be, a fascinating story to watch.

Have questions or tips?
Want to share your experience?
Connect with us on:

ABOUT ▶

About

Global Payments Made Easy.

A worldwide leader in payment services, 2Checkout maximizes online sales conversions by giving global buyers localized payment options. Trusted by over 50,000 merchants, 2Checkout supports transactions in 196 countries through 8 payment methods, 26 currencies, and 15 languages, forming one of the leading processors of online transactions in the world.

Connect with 2Checkout and learn more about how our services can enable you to implement these principles.

Connect >>

Thomas Kossler

is a 40-year veteran of the credit card industry, having worked with both private-label and general purpose card programs, ATM networks, and with most major acquirers. Mr. Kossler is a former member of the 2Checkout board of advisors.