Merchant Acquirers and Payment Card Processors: A Look inside the Black Box

RAMON P. DEGENNARO

The author is the SunTrust Professor of Finance at the University of Tennessee and a visiting scholar at the Federal Reserve Bank of Atlanta. *He thanks Jerry Dwyer, Dick Fraher, Scott Frame, Will Roberds, and Lynn Woosley for useful comments and discussions. He is grateful to Timothy Miller and Mario Beltran of NOVA Information Systems for explaining important institutional details and to Lee Cohen and Victoria L. Messman for research assistance.*

Like most consumers, you probably take your credit and debit card transactions for granted. You and others like you carry millions of cards and use them billions of times annually. But unless a transaction goes awry, you rarely think about how your cards work. In fact, a great deal happens after you produce your card to pay for a purchase and before the merchant receives funds and you receive your bill.

What happens during the few seconds between the time you swipe your card and the terminal flashes a result? How does that swipe translate into a line on your bill from the institution that issued the card? When making a purchase using a card online or over the telephone, why are you sometimes asked for the three- or four-digit number printed on the back of the card, the card's expiration date, or arcane information such as your mother's maiden name?

From the merchant's perspective, how is that same card swipe turned into cash to pay for the goods or services provided? Why does a merchant pay a larger fee when it accepts a card in some circumstances than it does in others? And why was the representative from the payment card company so interested in the merchant's personal information before the merchant was even permitted to accept cards?

This article answers such questions. It explains how the card network signs up merchants to accept payment cards and how the sales slips that consumers sign are converted into cash for the merchants. The discussion begins with an explanation of the simplest type of card transaction—one using a private-label card (one that is accepted by only one merchant)—but the focus is primarily on the Visa and MasterCard networks in the United States. The major aspects of payment cards are similar in other countries, although details may differ, especially for cards other than Visa and MasterCard. The key institutions in this transactions process are the merchant acquirer and the payment card processor. The largest of these often perform both functions. Together, merchant acquirers and processors serve as the communications and transactions link between the merchants and the card issuers.

Merchant acquirers and card processors are important for several reasons. First, every card issuer deals with at least one payment processor, and every merchant that accepts cards has a relationship with a merchant acquirer. Without them, the payment system as we know it would not exist. According to Gerdes et al. (2005), U.S. consumers used credit cards for 19 billion transactions and debit cards for another 15.6 billion in 2003. These figures represent a dollar volume of $1.7 trillion for credit cards and $600 billion for debit cards. In terms of dollar value, annual growth for credit cards between 2000 and 2003 was 9.9 percent, and for debit cards, 21.9 percent. According to the *Nilson Report* (2005a), in 2004 consumers in the United States held 795.5 million MasterCard and Visa cards (about three cards for every man, woman, and child in the country).

Unbeknownst to the cardholder, card-based transactions actually travel through the Black Box—a highly evolved group of intermediaries.

Second, the industry generates revenues through merchant fees, which merchants must recover either through higher prices or more sales, and the dollar amount is substantial. Lucas (2004), for example, reports that debit and credit card fees are the fourth-largest expense for gas stations and convenience stores after labor, rent, and utility costs.

Third, the merchant acquiring and processing industry employs many workers. Jeff Johnson, vice president of search and recruitment with CSH Consulting, estimates that the industry employs about 50,000 people.[1] Despite the size of the industry, few people understand the function of merchant acquirers and processors, and almost no academic research on this topic exists.[2]

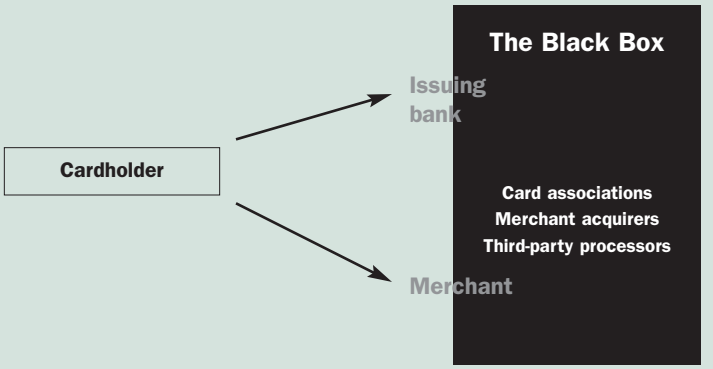
The next section describes how regulations and card association rules set the boundaries of the Black Box. A description of a private-label transaction follows. This is the simplest type of card transaction because the card is accepted by only one merchant. The article then identifies some major types of institutions in the payment card industry and traces the transactions process. The following sections describe how chargebacks and fraud affect a merchant acquirer and identify cross-sectional risk differences among card transactions from the perspective of the merchant acquirer.

The Boundaries of the Black Box

Figure 1 presents a schematic of a credit and debit transaction, in which the cardholder is typically aware only of the issuing bank and the merchant. The cardholder deals with the issuing bank and with the merchant under the protection of Regulations Z and E. The issuing bank and the merchant are liminal figures that deal with the cardholder in the realm of these regulations and with the Black Box through the associations and the merchant acquirers. Unbeknownst to the cardholder, card-based transactions actually travel through the Black Box—a highly evolved group of intermediaries that sign up merchants to accept cards, handle card transactions, manage the dispute-resolution process, and, along with regulatory agencies, set rules that govern card transactions.

Things can and do go wrong with card purchases and billings. Sometimes the culprit is poor quality or bad service. Sometimes the merchant fails to deliver the product. Cardholders and merchants may dispute a refund, and fraud by both cardholders and merchants is a constant challenge. Although these matters can cause serious headaches for cardholders and issuing banks, in most cases the financial impact is relatively minor from the cardholder's perspective. This situation exists because Regulation Z and card association rules limit an innocent cardholder's liability to at most $50 in

Figure 1
The Boundaries of the Black Box



Cardholders generally interact with the Black Box only through merchants and issuing banks.

almost all cases involving credit card fraud, and Regulation E and association rules provide essentially the same protection for debit card users.[3] Regulations Z and E thus shift liability for fraud from the (innocent) cardholder to other parties. By means of contracts, the parties within the Black Box and the issuing banks assume and allocate this liability.

In practice, then, Regulations Z and E ensure that most of the losses that result from card-based transactions are allocated among the entities within the boundaries of the Black Box. Aside from initiating a transaction with a merchant at the point of sale, the only time a cardholder interacts with the Box itself is during a dispute. Even then, if an attempt at resolution between the cardholder and the merchant fails, the cardholder typically turns to the issuing bank for relief. For their part, issuing banks usually interact with the Black Box only through the card associations.

Private-Label Cards

This section describes a simplified example of a transaction using a private-label card—a card accepted only by the merchant that issued it. Examples include department stores such as Macy's and Sears. The transaction begins when the consumer presents the card at the point of sale. The sales clerk enters the purchase amount and, depending on the equipment available, either records the card number and obtains a signature or swipes the card. Depending on the specific merchant, the rest of the transaction cycle is handled either in-house or by a third party such as GE Capital. Sears handled its own processing until 2003, when it sold that part of its business to

1. Jeff Johnson, e-mail messages and telephone conversations with author (November and December 2005).
2. An exception is Rochet and Tirole (2002). Their focus differs from this article's. They develop a theoretical model of optimal interchange fees and the merchants' decision to accept payment cards.
3. Section 226.13 of Regulation Z addresses credit card "billing errors." Section 205.11 of Regulation E contains error-resolution procedures for debit cards, and Section 205.6 of Regulation E covers consumers' obligation for unauthorized transfers.

Table
The Ten Largest U.S. Merchant Acquirers in 2004, Excluding Partnerships and Alliances

Ranking (transactions)	Ranking (dollar volume)
1. First Data	1. Chase Merchant Services
2. BA Merchant Services	2. BA Merchant Services
3. Chase Merchant Services	3. First Data
4. Paymentech	4. Paymentech
5. Fifth Third Bank	5. Nova Information Systems
6. Global Payments	6. Fifth Third Bank
7. Nova Information Systems	7. Global Payments
8. Wells Fargo	8. Wells Fargo
9. Alliance Data Systems	9. First National Merchant Solutions
10. Heartland Payment Systems	10. Heartland Payment Systems

Merchant acquirers holding at least 1 percent of U.S. market share in 2004 (by dollar volume), including partnerships and alliances

1. First Data (including Chase Merchant Services, Paymentech, Wells Fargo, SunTrust, and PNC)
2. BA Merchant Services
3. Nova Information Systems (including KeyCorp)
4. Fifth Third Bank
5. Global Payments
6. First National Merchant Solutions
7. Heartland Payment Systems
8. TransFirst

Source: *The Nilson Report* (2005b)

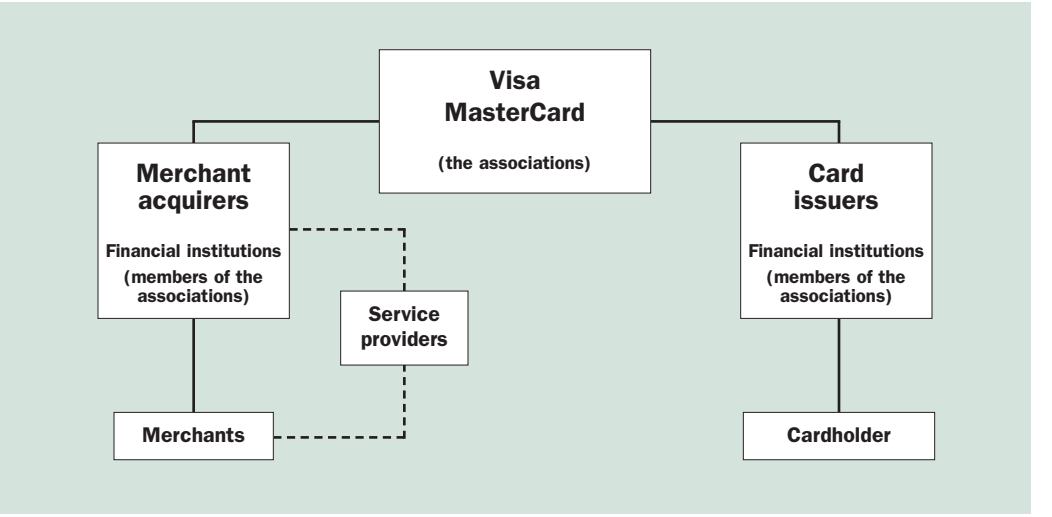
Citigroup. In this simplified example, the processor bills the cardholder and remits funds to the merchant.

Private-label transactions are relatively simple because only one merchant and one processing entity are involved. For universal cards such as Visa and MasterCard, the situation is more complex not only because many different merchants could have made the sale but also because many different banks could have issued the card. Specialized institutions have evolved to route transactions to the correct business entities, and others have evolved to manage the relationship between the card networks and the merchants.

Payment Cards: The Industry and Transactions Processing

The industry. The payment card industry comprises many different entities that perform various tasks, and because many of them have formed alliances, the lines between them are often blurred. The card issuer provides the cards to the consumer and, in the case of credit cards, extends credit to the consumer. (See the sidebar on page 32 for information about different types of cards.) The relationship is business-to-consumer. The merchant acquirer signs up merchants to accept payment cards for the network. This relationship is business-to-business. These acquirers also arrange processing services for merchants. Processors handle transaction authorization and route a (usually electronic) transaction from the point of sale to the network (front-end processing). Later, they handle the information and payment flows needed to

Figure 2
Parties Involved in a Card Program: A Four-Party Network



convert the electronic record created at the point of sale into cash for the merchant (back-end processing). Some merchant acquirers perform the processing themselves; others resell the services of a third-party processor. That is, they are merchant acquirers who resell front- and back-end processing services but do not provide those services themselves. Most of the larger merchant acquirers also function as processors, but almost all of the smaller ones are resellers. The table lists the ten largest merchant acquirers by the number of transactions processed and by dollar volume. Because some acquirers have formed partnerships and alliances, the table also reports the eight groups with more than 1 percent of U.S. market share (by dollar volume).

Only a bank may join Visa or MasterCard; as a result, many merchant acquirers and processors form an alliance or partnership with a sponsoring bank. In addition, depending on the needs of the merchant, an acquirer might sell front-end processsing from any of several companies and back-end processing from yet another one. These arrangements make the web of relationships messy, complicating the transactions process. The next section clarifies this process.

Transactions processing. Figure 2 illustrates the institutions participating in a transaction involving either of the two major payment card associations, MasterCard and Visa, which are examples of four-party networks.[4] The network includes the card issuers and the merchant acquirers/processors plus the cardholders and the merchants. The card issuer distributes cards to consumers, bills them, and collects payment from them. The merchant acquirer recruits merchants to accept cards and provides the front-end service of routing the transaction to the network's processing facilities. The processor is responsible for delivering the transaction to the appropriate card issuer so that the customer is billed and the merchant receives funds for the purchase. Acquirers often delegate the actual processing to third-party service providers. The sidebar on page 36 provides a brief explanation of the differences between four-party networks and three-party networks (for

4. The associations, as umbrella organizations, are not counted as a separate group. Neither are service providers because their function is often served by merchant acquirers.

Types of Payment Cards

Consumers today can choose from a wide variety of payment cards, and the universe of cards can be partitioned in several ways. For example, one way to differentiate cards is according to the merchants who accept them. Some retailers issue private-label cards that are accepted only in their stores. Examples include Sears and Macy's. General-purpose cards, by contrast, are accepted by a wide variety of merchants. Visa and MasterCard are the most common examples.

Another way to classify payment cards is by the amount of time consumers have before payment is due. Debit cards enable a direct withdrawal from the user's savings or checking account, and payment is due much sooner than for a credit or charge card. Debit cards can be used in either online or offline mode. When used in online mode, the card is swiped through a terminal equipped to handle a personal identification number (PIN). In this case, the cardholder enters a PIN instead of signing a transaction slip, and funds are deducted from the user's account immediately. In offline mode, the card is swiped through a standard terminal, and no PIN is entered. Instead, the merchant obtains the cardholder's signature. In this case, the customer's account is debited within two or three days. A debit card user can purchase any amount up to his balance in that account, and some of these cards even come with overdraft protection.

In contrast, credit cards and charge cards allow the purchaser a longer period of time before he must deliver funds to cover the purchase, and the card may or may not have a predetermined spending limit. Charge cards require the cardholder to pay the balance in full each month unless special arrangements have been made while credit cards allow him the option to make only a minimum payment and pay interest on the balance carried from month to month.

Still another way to distinguish payment cards is by the type of issuer. Financial institutions issue bankcards, which may be either charge cards or credit cards. Visa and MasterCard are the most popular examples. Nonfinancial institutions issue non-bankcards. Market participants subdivide these non-bankcards into two subcategories. Nonbank credit cards, such as Discover Card, enable the cardholder to roll over a balance from month to month while some travel and entertainment cards, such as the American Express Rewards Green Card and the Diners Club Charge Card, are charge cards.

example, American Express, Discover Card, and Diners Club), in which the card issuer and merchant acquirer are the same entity.

The transactions process has two major parts. The first is authorization, and the second is clearing and settlement. Authorization is the process of obtaining permission from the bank that issued the card to accept the card for payment. Clearing and settlement is the process of sending transactions through the Visa or MasterCard network so that the merchant can be paid for the sale. Authorization begins when a consumer presents his card to the merchant for a purchase. Usually, this authorization happens at the point of sale, though an increasing number of transactions are being done in "card not present" situations (for example, online). Merchants usually obtain authorization electronically, either by having the consumer swipe the card through a terminal at the point of sale or by entering the card information manually. However, some transactions still rely on voice authorization, which entails the merchant calling an authorization center to obtain permission to accept the card.[5] The terminal sends the merchant's identification number, the card information, and the transaction amount to the card processor. The processor's system reads the information and sends the authorization request to the specific issuing bank through the card network. The issuing bank conducts a series of checks for fraud and verifies that the

cardholder's available credit line is sufficient to cover the purchase before returning a response, either granting or denying authorization. The merchant acquirer receives the response and relays it to the merchant. Usually, this process takes no more than a few seconds.

After authorization, the second major part of the transactions process—clearing and settlement—begins. When a consumer purchases an item with a payment card, the consumer and the merchant form a contractual obligation. The merchant agrees to deliver the goods or services, and the consumer agrees to pay for them. Settlement is the process by which assets are delivered to discharge that obligation. Clearing comprises the series of transaction activities from the moment the trade or purchase occurs until it is settled. Usually, clearing involves the transfer of information rather than assets. Examples include netting numerous trades to reduce the number of deliveries, meeting reporting requirements, or handling failed trades (say, due to an error in recording). In the payment-card industry, the most common example of clearing is the process of transfering transaction information from the merchant to its bank. Clearing, then, includes activities that facilitate settlement.

Specialized institutions have evolved to route card transactions to the correct business entities, and others have evolved to manage the relationship between the card networks and the merchants.

In practice, clearing and settlement for payment cards is more complicated because several entities are involved. Recall that payment card networks include four distinct parties (Figure 2). Moreover, each of those parties for a transaction could be one of hundreds or thousands of different acquirers or issuers and one of millions of cardholders or merchants. The process differs somewhat depending on the specific merchant acquirer and the type of network. The following discussion outlines the major steps of a typical clearing and settlement process for payment cards.

Figure 3 illustrates a typical transaction cycle. In the first step, the merchant sends its transactions to its merchant acquirer. The merchant acquirer sends this information to the merchant accounting system (MAS) servicing that particular merchant's account. In some cases, the MAS is a part of the merchant acquirer; in others, it is a different entity. The MAS distributes the transactions to the appropriate network—Visa transactions to the Visa network, MasterCard transactions to the MasterCard network, and so forth.[6] Next, the MAS deducts the appropriate merchant discount fee (to cover the costs of the merchant acquirer's activities) from the transaction amount and generates instructions to remit the difference to the merchant's bank for deposit into the merchant's account. The MAS sends these instructions to the automated clearinghouse (ACH) network, which is a computer-based system used to process electronic transactions between participating depository institutions.[7]

---

5. For authorization of card-not-present transactions, merchants must follow procedures designed to minimize error and fraud. For example, merchant acquirers can require use of the Address Verification Service (AVS). AVS offers varying levels of detail, including the cardholder's ZIP code, street, city, or state. AVS can even verify which bank issued the card; if the buyer can provide that information, then he probably has the card in hand. This verification process helps rule out fraud by someone who has stolen the card number and does not have the card itself.
6. The process for transactions routed to networks other than MasterCard or Visa is somewhat different than the one that follows in the text, particularly regarding the handling of payments.
7. FedACH is part of the Federal Reserve System; the Electronic Payments Network (EPN) is the most notable example of a private ACH network.

To recover these funds, the MAS sends information about the merchant's transactions to Interchange, which is part of the Visa or MasterCard network. Interchange is the clearing and settlement sytem that transfers data between the card processor and the issuing bank. Interchange determines the interchange fee and Visa/MasterCard assessments (to cover the cost of the issuing bank's services and the network's costs) and sends the information to the card-issuing bank. In turn, the issuing bank remits the transaction amount, less the interchange fee, to Interchange, which passes it on to the MAS. Finally, the issuing bank bills the cardholder and collects the balance.[8]

Merchant acquirers provide other services to merchants besides the processing described above, including installing card terminal equipment, recording transactions, providing reports, and handling problems with card processing (Chang 2004). Some acquirers also provide related services such as analyzing the purchasing patterns of the merchant's customers.

Chargebacks and Fraud

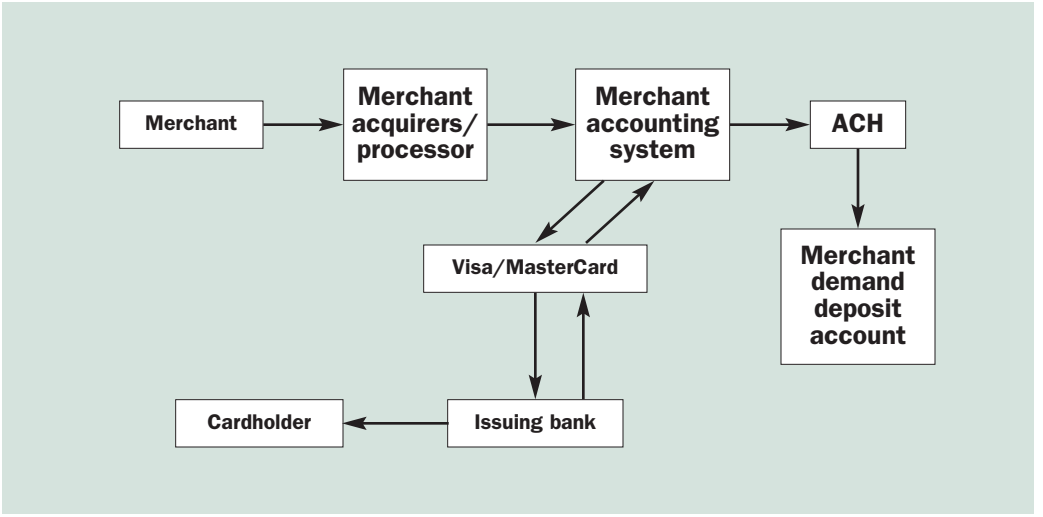
Chargebacks. A merchant acquirer suffers losses if a merchant is unable to make good on credit transactions disputed by customers, called chargebacks. Chargebacks usually occur when a consumer is dissatisfied with a product or service. Beginning with the later of the date on which a transaction is processed or the delivery of the product or service, cardholders have as much as three months to claim a chargeback—sixty days plus up to another month depending on the purchase date relative to the billing cycle.[9] The presumption is initially in favor of the customer, and the amount of the chargeback is deducted from the merchant's account pending the result of a review. If the dispute is resolved in the merchant's favor, then the merchant recovers the funds. The merchant acquirer is at risk in the event that the merchant fails between the time of the initial sale and the time his account is debited for the chargeback. In this case, according to the card network's rules, the merchant acquirer is liable and must make restitution to the customer.

Because of this feature, the merchant (and ultimately the merchant acquirer) is at risk of loss for up to several months because the transaction can be reversed. In the language of payments, the transaction is not final. This feature greatly enhances the appeal of credit cards to cardholders, but it also shifts the risk of chargebacks to the merchant acquirer. In essence, the merchant acquirer has insured the issuing bank against an adverse result. The risk of a merchant acquirer's contingent liability is similar to that of a bank's guarantee of a debtor's liabilities or an insurance contract. Merchant acquirers include the cost of this implicit insurance in the price that merchants pay for their services.

Quinn and Roberds (2003) argue that payment-finality rules are essentially loss-allocation rules. The rules determine which party to a transaction absorbs the loss if the transaction is not completed. For example, cash transactions are final when goods or services are exchanged for cash. Absent fraud or a private agreement such as a warranty, neither the buyer nor the seller can cancel the transaction after the exchange. In contrast, because of Visa/MasterCard chargeback provisions, credit card transactions are effectively not final for up to three months after delivery of the good or service. This lack of finality is a key determinant of a merchant acquirer's risk because, until a transaction is final, the merchant acquirer bears the risk that a merchant cannot cover a chargeback.

The industry attempts to quantify this risk through the closely related concept of delayed delivery. Magazine subscriptions are a good example. Subscribers pay for subscriptions in advance, and the term of subscriptions can be as much as a few

Figure 3
The Transactions Process



years. If the magazine ceases publication before the term of the contract, then the subscriber has recourse for undelivered issues according to Visa/MasterCard rules. The delay between the sale and the delivery of the goods or services increases the chances that the merchant will fail and be unable to cover the resulting chargeback. The sidebar on page 38 describes an extreme example.

Fraud. Kahn and Roberds (2005) define fraud risk as the risk that a claim cannot be collected because the identity of the person who incurred the debt cannot be established. They identify three distinct types of fraud. First, existing account fraud is usually traced to stolen account information. For example, a thief who steals a card and orders merchandise commits existing account fraud. The second category is new account fraud, popularly called identity theft. In this case, a thief uses information about a third party to open an account, incurring debts in the name of the victim. Finally, those who commit friendly fraud make legitimate transactions that they later deny having made.

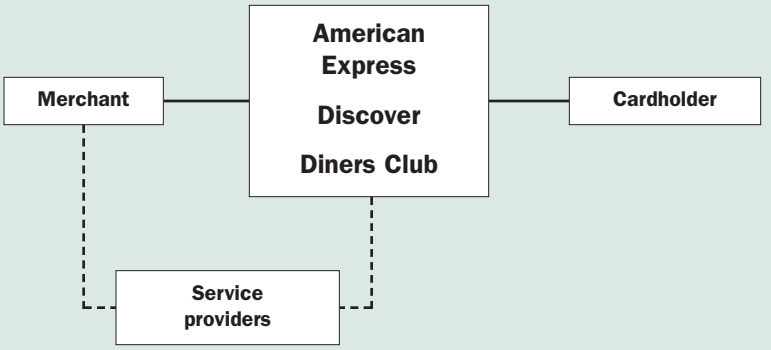
The risk of fraud is especially serious if a merchant takes orders by mail, telephone, or over the Internet. In such card-not-present situations, the Truth in Lending Act frees cardholders from liability—they are not responsible for even the first $50 (association rules provide essentially the same protection for debit card users). This consumer protection shifts the risk to merchants and, in turn, creates a larger contingent liability for merchant acquirers. One notorious example involves a merchant that defrauded customers by taking orders with no intention to deliver. Had the merchant been a traditional storefront operation, red flags would have been more apparent. First, customers would have been interacting with the merchant face to face,

8. For debit cards, the billing is done automatically. Put differently, the cardholder's account is debited, and the cardholder later receives a statement of transactions rather than a bill.
9. Specific details of chargeback terms are complicated because they are governed by law (for example, the Truth in Lending Act), by regulation (Regulation Z for credit cards and Regulation E for debit cards), and by the rules of the card associations and networks. See Furletti and Smith (2005) for more information. The terms in the text are common in the industry.

Three-Party Networks

The figure illustrates the three-party analog to the four-party diagram in Figure 2. The only major distinction is that, in three-party networks, the card issuer and the merchant acquirer are the same entity; in four-party networks, they are separate. In four-party networks, banks that are members of Visa and MasterCard issue the payment cards and extend credit to consumers for credit cards. Separate entities are responsible for signing up merchants to accept these cards for payment. In practice, some acquirers are affiliated with or have formed partnerships with card issuers. Most payment cards in three-party networks are nonbank cards, issued by institutions such as American Express, instead of a bank. In almost all cases, the difference between three- and four-party networks is unimportant for cardholders.

Figure
Parties Involved in a Card Program: A Three-Party Network



making it easier to detect suspicious behavior. Second, customers would have been more likely to benefit from the experiences of other customers; they might have met in the store or overheard conversations and complaints. Finally, either the merchant would have had no inventory or business history at that location (fueling suspicion), or he would have had at least some inventory and other collateral after the firm failed. Either way, the merchant acquirer would have been better off. Instead, because this was a card-not-present situation, the fraudulent merchant was able to collect a large amount over a period of several weeks. When consumers were no longer willing to wait for delivery and filed chargebacks, they were entitled to relief. Because the fraudulent merchant could not pay, the merchant acquirer was forced to make restitution.

Cross-Sectional Risk Factors

Clearly, a merchant acquirer must consider the credit standing of the merchants it services. Merchant acquirers do perform credit analysis, but the analysis is different from that of a more familiar bank loan. A merchant acquirer's contingent liability is more similar to an insurance contract than to a bank loan. This description fits in part because the acquirer pays only if another entity cannot, but there are other differences. For example, for a bank loan, the bank delivers funds to a borrower. A merchant acquirer, though, advances no funds. Instead, it indemnifies a third party—the card

issuer (who in turn indemnifies the cardholder)—in the event that a merchant cannot cover a chargeback.

Another major difference between bank loans and a merchant acquirer's contingent liability is the term of the contract. Bank loans can have maturities of several years. In contrast, although consumers can file chargebacks for up to several months after a purchase, the effective term of the contingent liability produced by each transaction is usually measured in a very few days. In addition, merchant acquirers review most accounts at least once a year. Cast in terms of the probability of default times the loss given default, the probability of default is affected in part by the time between account reviews, and the loss given default—again absent delayed delivery—rarely represents more than a few days' worth of total processing volume at any one time.

Because the merchant acquirer is at risk if the merchant cannot cover a chargeback, the acquirer must evaluate the credit quality of merchants seeking or using the acquirer's services.

Taken together, the merchant acquirer's annual review of accounts and the short term of the contingent liability have enormous implications for risk. The annual review makes the risk that merchant acquirers face similar to a short-term bond, whereas a bank loan is (sometimes) more similar to a long-term bond. Investors in short-term bonds need not reinvest in the same company when their bonds mature if, for example, a company's credit quality deteriorates. Long-term investors do not have that option. They can only sell their bonds prior to maturity, likely taking a loss because the credit standing of the bonds has deteriorated. Similarly, if a merchant's credit quality deteriorates, a merchant acquirer need not renew the relationship, whereas a bank probably cannot cancel a loan unless a covenant has been violated.

Because the merchant acquirer is at risk if the merchant cannot cover a chargeback, the acquirer must evaluate the credit quality of merchants seeking to use the acquirer's services and monitor the credit quality of the merchants it currently services. The acquirer considers industry effects, firm-specific effects, and even the nature of individual transactions. In fact, merchant acquirers charge different fees depending on whether or not a merchant has followed certain procedures for a transaction.

Industry effects. Because customers who regret making a purchase have up to three months to act before their credit card purchases are final, businesses that are susceptible to so-called buyer's remorse present higher risk to a merchant acquirer. Consider health clubs, which often sell annual memberships at a discount relative to their monthly fee to encourage customers to commit for a longer period. The problem is that many customers regret their commitment after just a few weeks. Although buyer's remorse alone is not sufficient to win a chargeback dispute, it does give the buyer incentives to try to exploit the process. For example, he might claim that equipment at the club is often broken or that the premises are unsanitary. Because "often" and "unsanitary" are matters of degree, the cardholder has a chance to win the chargeback dispute, putting the acquirer at risk. Merchants that sell items of high and uncertain value—collectibles are an obvious example—are also prone to customer disputes. Customers can be disappointed in artwork, rare coins, or stamps for any of several reasons. Also, fraud is frequently involved in these types of businesses because the goods may not be genuine or their condition might be exaggerated. Mystics, such as fortune tellers, face high chargebacks due to buyer's remorse, and one can easily see how customers of gambling establishments could regret a transaction depending on the outcome of a race or sporting event. For this reason, such businesses usually are not authorized to take credit cards for purchases.

Delayed Delivery in the Extreme

The nature of airline ticket sales and the industry's current financial problems combine to form an extreme example of delayed-delivery risk. Consider a cardholder planning a trip by air. In some cases, the cardholder buys his ticket weeks or even months in advance, and travelers usually pay for their tickets using a credit card. Suppose that the airline fails between the time of purchase and departure. In this case, under credit card association rules, the acquirer must make restitution. How large can the potential losses be?

One merchant acquirer, National City Corporation, reports that as of June 30, 2004, the value of credit card transactions it had acquired for outstanding tickets purchased on United Airlines was $853 million (National City Corporation 2004a). United Airlines is operating under Chapter 11 protection as of this writing. If United Airlines were unable to honor those tickets, then travelers who purchased their tickets using credit cards would be entitled to refunds under Visa and MasterCard rules, and National City held no significant collateral against this potential liability as of June 30, 2004. The $853 million worth of unflown tickets, of course, represents the potential liability from exposure to United Airlines alone. National City Corporation (2004a) says that it processed over five times that amount—about $5 billion worth of delayed-delivery purchases—during the six months ending June 30, 2004. National City Corporation (2004b) reports that as of December 31, 2004, the value of unflown tickets had been reduced to $547 million.

Of course, the odds are small that National City Corporation would be liable for the full amount of these huge sums. Consider the case of United Airlines. For National City Corporation to be liable for the full amount, three things must happen. First, United Airlines must halt all flights. Second, all ticket holders must file chargebacks within the allotted time limits. Although this is within their rights, many travelers would instead opt to fly on other airlines, which usually honor the stranded travelers' tickets on a standby basis (McCartney 2004).[1] This provision reduces the number of travelers who file chargebacks. Finally, National City Corporation would have to have a recovery rate of zero in liquidation. This outcome is unlikely because, even as a general creditor, the company could probably recover a portion of its losses from the bankrupt carrier. If National City Corporation anticipates problems it can also require a security deposit, a line of credit from a bank, or delay payment to the merchant.

National City Corporation (2004a) puts the problem in perspective. For the first and second quarters of 2003 and 2004, the company processed about $35 million in chargebacks each quarter, for a total of about $150 million in the four quarters. Actual losses were about $1 million each quarter, for a total of about $4 million. The company had $5 million worth of chargebacks in the process of resolution as of June 30, 2004. The company believes the chance of a "material loss" because of chargeback rules is "unlikely" (National City Corporation 2004a). Still, losses of this size are not trivial, and "unlikely," of course, does not mean that a material loss is impossible.

1. In November 2005, Congress extended this provision through November 2006. Airlines must honor these tickets but may charge a fee and need only accommodate travelers on a space-available basis.

Instead, customers must get cash advances on their cards and use the cash to make the purchase.

Items that can easily be resold are prone to fraud, so dealers in these products also present higher risks. Consumer electronics and jewelry head the list. Intangible products, particularly downloadable software, tend to attract fraudulent merchants and customers because proof of delivery and the products' performance are difficult to substantiate. Timeshare services have high chargeback rates because customers sometimes place deposits months before developers even begin construction, when

the suitability of the property is difficult to ascertain. Customer dissatisfaction is more common in such cases.[10]

Perhaps the best example of an industry effect is the restaurant industry. Most bankers realize that loans to restaurants are very risky. For example, the Cline Group (2003) tracked over 4,000 non-fast-food restaurants in the Dallas area and reported that an average of 23 percent failed during their first year. Yet restaurants are extremely safe customers for merchant acquirers. Why? Consider the nature of a restaurant transaction. The diner finishes the meal, pays using a credit card, and departs. In the vast majority of cases, the consumer is satisfied enough to consider the transaction to be final, and the settling of accounts proceeds normally. Suppose instead that the diner is dissatisfied. Although Visa/MasterCard rules give the diner the right to file a chargeback for several weeks afterward, only in very rare circumstances will the diner pay, leave the premises, and then file a complaint. The diner is more likely to voice his dissatisfaction during the meal, and, almost always, restaurant management accommodates the diner. By the time the consumer uses his credit card, he is satisfied and considers the transaction to be final. The settling of accounts again proceeds normally. Only in very rare circumstances will he still complain after using his credit card. Even then, a complaint does not necessarily imply that the acquirer bears a loss. For the merchant acquirer to incur a loss, the cardholder must win the chargeback dispute (unlikely in such cases), and the merchant must fail between the time of the sale and the chargeback. Otherwise, the merchant itself and not the acquirer is responsible for the chargeback.

Because customers who regret a purchase have up to three months before their credit card purchases are final, businesses that are susceptible to so-called buyer's remorse present higher risk to a merchant acquirer.

Firm-specific risk. Just as insurers and banks evaluate the credit risk of individual companies, so do merchant acquirers. For example, they study standard measures of financial strength, such as financial ratios of individual firms. For unincorporated businesses, financial statements are often unaudited, so acquirers might use business tax returns to supplement the unaudited statements. Especially for small firms, acquirers even proceed beyond the firm level and use information about the owners and managers of companies, especially for unincorporated businesses. Acquirers can use credit scores from the Fair Isaac Corporation, commonly known as FICO scores, at the personal level as well as at the business level. Acquirers also use credit report information and the number of years that a potential customer has been in business to gauge risk. Both traditional lenders and merchant acquirers use information that others have already generated about specific firms—for example, whether or not the merchant has existing banking relationships. Almost surely, an international company will receive greater scrutiny than a domestic one. The processing history of a company that already has a relationship with a merchant acquirer is always important, particularly fraud and chargeback rates.

If the firm's condition is sufficiently weak, a merchant acquirer might require the owner to offer a personal guarantee; such guarantees are common for small business loans. An acquirer might impose conditions similar to restrictive covenants in business loans. For example, the acquirer might impose a processing limit, which corresponds to a commercial bank's lending limits. Like a bank, the acquirer might require

10. For examples of items on restricted lists, see www.internetsecure.com/solutions-faq.htm#2 and www.practicepaysolutions.com/apply/index0007.php.

marginally qualified merchants to provide collateral, usually in the form of a certificate of deposit, cash, or a letter of credit. If the merchant cannot provide collateral, then the acquirer might institute a holdback, or a delayed-payment arrangement. Under such an arrangement, the merchant acquirer withholds payment to the merchant for a predetermined length of time after processing. The duration of the payment delay is usually a function of the delivery delay and, less frequently, the chargeback ratio.

Transaction-related risks. Banerjee (2004) notes that credit cards were originally designed to be physically present at the point of sale. If merchants followed procedures, then nearly all risks except fraud and delayed delivery declined enormously. This low level of risk is still true for face-to-face transactions. For example, if a merchant swipes a card instead of manually keying the card number, the chance for error drops to near zero. True, the card may have been stolen, but swiping is at least one step toward insuring legitimacy: A thief must have stolen the card itself and not just the card number. This consideration goes far toward eliminating theft losses from, say, a dishonest waiter who copies the card number while clearing a diner's tab.

These procedures are only partially effective, so merchant acquirers charge higher fees for card-not-present transactions to compensate for the higher risk.

For a growing number of transactions, however, the cardholder and the card are not present. As a result, merchants and merchant acquirers face the challenge of developing new procedures for limiting risk. Mail-order and telephone-order (MOTO) transactions—and, more recently, Internet transactions—have presented special problems for payment card associations. The most popular approach has been for merchants to have access to increasingly arcane bits of information during authorization. Some help to confirm that the purchaser has possession of the card itself and not just the card number. For example, card associations have long encoded a verification number into the magnetic stripe on the back of the card. Visa calls this code the Card Verification Value (CVV or CVV1); MasterCard's term is the Card Validation Code (CVC or CVC1). This code, read during the swipe, confirms that the card is actually present at the point of sale. The problem is that this approach cannot help for Internet or MOTO transactions because the card is not present and a swipe is impossible.

Associations have had to devise other ways to confirm that the purchaser is in physical possession of the card at the time of the sale. The result is CVV2 and CVC2. These three-digit numbers (different from the magnetically coded CVV or CVC numbers) are printed on the right side of the signature area on the back of the card. Because this number is not embossed on the card, it does not appear on a paper sales slip, making it harder to steal. The customer must have physical possession of the card—or the printed number stolen by some other means—for the buyer to have access to it. CVV2 and CVC2 are only partially effective, though. First, the network merely flags the transaction if the buyer cannot provide the number; it does not refuse it. Second, some situations make it easy to defeat. For example, a dishonest waiter can steal a CVV2 or CVC2 number while clearing a dinner tab just as easily as he can steal a card number. Because these procedures are only partially effective, merchant acquirers charge higher fees for card-not-present transactions to compensate for the higher risk.[11] Still, CVV2 and CVC2 provide one more layer of protection, and Banerjee (2004) reports that they do help discourage fraud.

Another approach is to prearrange a question and answer or series of questions and answers. Card users might be asked to verify their mother's maiden name, for example. By allowing cardholders to select from a list of questions, merchants and

acquirers make it more difficult for a thief to have the necessary information. The Address Verification Service (AVS) is a good example (see footnote 4). This verification process helps rule out fraud by someone who has stolen the card number and does not have the card itself. These procedures are somewhat effective, but as Banerjee (2004) points out, none of the ways to reduce fraud on the Internet seems to be particularly effective. As evidence, he notes that issuers have not lowered the interchange fees they charge for transactions that follow these procedures. More recent innovations are Visa's Verified by Visa and MasterCard's MasterCard SecureCode. Both of these systems use passwords for Internet purchases to insure that only the cardholder can make such purchases.

These examples illustrate that merchant acquirers can help protect merchants (and therefore themselves) from fraud by setting procedures. After all, most merchants are too small to dedicate resources to designing low-cost, effective fraud-protection procedures, so a merchant acquirer can add value by supplying them. Merchant discount rates provide a means for acquirers to give incentives without mandating a specific procedure for each different merchant.

Merchant acquirers provide these incentives by setting qualification levels for the discount fee that merchants pay; the more hurdles the merchant surmounts for a transaction, the higher the qualification rate and the lower the discount fee. A three-tiered system is common, beginning with the nonqualified rate, which is the lowest acceptable category (with the highest fee); moving to the partially qualified rate; and ending with the qualified rate, which is the highest category. For an example of how these tiers are determined, consider the method of entering the card number. Being hand-keyed without AVS might automatically drop a transaction to the nonqualified rate; adding AVS might move the transaction to the partially qualified rate. Swiping the card could move the transaction into the qualified rate.

Different industries sometimes have different qualification criteria. For example, tipping is common in businesses such as restaurants, and the amount of the tip is usually unknown until after the card is swiped or the card number is entered. Therefore, the amount approved is a lower bound on the total amount to be charged. If the final amount including the tip is sufficiently above that lower bound, then the transaction might drop to the partially qualified rate from the qualified rate.

A merchant acquirer's management of individual sales is not limited to the time when the customer places the order. Merchant acquirers often require merchants to follow specific procedures immediately prior to shipping. For example, just before shipping a back-ordered item, a merchant might be required to contact the buyer to verify the customer's telephone number, mailing and shipping address, or e-mail address. For MOTO or Internet purchases, shippers can insist that products be delivered only to the card's billing address (rather than delivering to a destination that a would-be thief designates). This practice helps reduce fraud because the thief is less likely to attempt fraud in the first place if he knows he may not receive the merchandise.

Finally, card associations have set procedures that force acquirers to cooperate to improve network efficiency. One obvious example is the MATCH list (Member Alert to Control High Risk Merchants), maintained by Visa and MasterCard, which comprises problem companies. If a merchant acquirer denies permission to accept cards to a merchant because of adverse processing behavior and fails to add it to the MATCH list, then the merchant acquirer is liable for losses another provider might suffer from that merchant.

---

11. For example, see AMS's Web site at www.merchant-accounts.com/retail-merchant-account.html.

Summary

Consumer and merchant acceptance of payment cards has been phenomenal. Hundreds of millions of cardholders make billions of transactions worth trillions of dollars each year. Yet few cardholders understand how payment networks operate. Most treat them as a Black Box.

This article demystifies the transactions process for payment cards, emphasizing the roles of the merchant acquirer and card processor. After outlining the regulations and card association rules that set the boundaries of the Black Box, the article describes a transaction with a private-label card. The discussion then considers the complications introduced by general-purpose cards, such as Visa and MasterCard, and introduces a key participant in the payment card market, the merchant acquirer. The description of the risks borne by merchant acquirers demonstrates that they take losses on these transactions only in rare circumstances—usually when a merchant fails to make good on a chargeback. The article also delineates some of the risk factors associated with specific industries, merchant types, and transactions that influence the price merchants pay for these transactions services. Finally, the article discusses some ways that merchant acquirers manage the risks that they face, especially the risk of fraud.

REFERENCES

Banerjee, Sankarson. 2004. Credit card security on the Net: Where is it today? *Journal of Financial Transformation* 12 (December): 21–23.

Chang, Howard H. 2004. Payment card industry primer. *Payment Card Economics Review* 2 (Winter): 29–46.

Cline Group. 2003. *Restaurant start & growth magazine unit start-up and failure study*. Cline Group for Specialized Publications, September.

Furletti, Mark, and Stephan Smith. 2005. The laws, regulations, and industry practices that protect consumers who use electronic payment systems: Credit and debit cards. Federal Reserve Bank of Philadelphia Discussion Paper No. 05-01, March.

Gerdes, Geoffrey R., Jack K. Walton II, May X. Liu, and Darrel W. Parke. 2005. Trends in the use of payment instruments in the United States. *Federal Reserve Bulletin* (Spring): 180–201.

Kahn, Charles M., and William Roberds. 2005. Credit and identity theft. Federal Reserve Bank of Atlanta Working Paper 2005-19, August.

Lucas, Peter. 2004. Why gasoline retailers are fuming. *Credit Card Management* (August): 20.

McCartney, Scott. 2004. Bill to protect flyers from shutdowns has a surprising beneficiary. *Wall Street Journal*, October 26.

National City Corporation. 2004a. *Form 10-Q: Quarterly report pursuant to section 13 or 15(D) of the Securities Exchange Act of 1934—for the quarterly period ended June 30, 2004,* Commission file number 1-10074. Filed August 6, 2004.

———. 2004b. Annual report.

The Nilson Report. 2005a. Visa & Mastercard—U.S. 2004. No. 828, February.

———. 2005b. Top U.S. acquirers. No. 831, April.

Quinn, Stephen F., and William Roberds. 2003. Are on-line currencies virtual banknotes? Federal Reserve Bank of Atlanta *Economic Review* 88, no. 2:1–15.

Rochet, Jean-Charles, and Jean Tirole. 2002. Cooperation among competitors: Some economics of payment card associations. *RAND Journal of Economics* 33, no. 4:549–70.