MERCHANT ACCOUNT AND PROCESSING 101

PLAYERS:

One of the most confusing parts of credit card processing (and the payments industry in general) is the sheer number of organizations involved with moving and handling transactions. Sometimes it's hard to believe how many players can be involved in a single transaction – especially when you consider the whole thing happens in less than three seconds.

Merchants/Merchant Banks:

Merchants You, the merchant, are an authorized acceptor of a credit card as payment for goods and services.

Merchant Banks (Acquiring Banks) Merchant banks, also known as acquiring banks, are the financial institutions where you have your merchant account. The merchant bank pays the fees owed to other banks and the card associations for transactions processed on behalf of its clients. In return, merchant banks are funded by the fee they charge you, known as the discount rate.

Merchant Services Providers (MSP):

A merchant services provider (MSP) is an independent organization authorized to set up your merchant account(s) and is responsible for all of your communications and relationships with card associations, processors, and merchant banks. Essentially, they act as extended sales forces for one or more merchant banks, bringing in merchant accounts to the banks that they work with.

Payment Gateways:

A payment gateway, like Jackrabbit is a third-party application service that protects cardholder data (CHD) throughout the payment transaction lifecycle in exchange for a fee per transaction. They route the communications between merchants and banks, processors, or other payment providers to ensure transaction information is passed securely in physical locations (e.g., retail stores) and e-commerce environments (e.g., websites).

Issuing Banks:

Issuing banks are the financial institutions that actually provide a credit card to a consumer (or business) for use. Issuing banks earn money through interest charged to the cardholders and, in some instances, through fees charged for the use of the card or access to rewards programs. Issuing banks also profit from a portion of the fees charged by the card association known as interchange fees.

Card Associations (Brands):

The card associations are the organizations behind the labels, or brands, on credit or debit cards, (e.g., Visa, MasterCard, American Express, and Discover). The card associations are responsible for following federal laws and statutes regarding all aspects of credit cards and their use, such as the Truth in Lending Act.

Processors:

Processors provide the connections necessary for the merchant to authorize and then settle credit card transactions. Every credit card transaction requires a front-end and a back-end processor (although they can

occasionally be the same organization). Front-end processors handle the upfront authorization of a credit card transaction. Back-end processors accept settlements from front-end processors and transfer the money from the issuing bank to the merchant bank via the Federal Reserve Bank (FED). Processors bill on a per-transaction basis, which is covered by the discount rate you pay to your merchant bank.

Now that you know who the main players are in processing credit card payments let's go over the basic process itself and how the players interact with one another during a transaction.

PROCESS:

Every time a cardholder presents his credit card to make a payment, an amazing amount of activity must take place to ensure that the merchant is ultimately funded for the transaction. Depending on the type of connectivity established between you and the processor, and which issuing bank is behind the card, all of this activity can take place in less than half a second.

AUTHORIZATION:

Merchants must obtain authorization for any transaction. Allowing merchandise to leave your store without first having authorization is a big risk. However, the many stages that comprise a transaction can make it difficult for clerks to know when they should allow a customer to leave with their purchase. Read on to see how authorization should take place and which responses you are likely to see from the bank.

1. A cardholder provides their credit card for payment.
2. Your clerk enters the card into a terminal, e-commerce kiosk, website, or other application by swiping the card through a device that reads the magnetic encoded information on the back of the card or by manually typing (keying) in the card number.
3. The card information, dollar value of the transaction, and specific information identifying you as the merchant is packaged, formatted, and sent electronically to your processor.
4. The processor identifies which brand is backing the card based on the first six digits of the card, commonly referred to as the bank identification number (BIN), then electronically routes the authorization request to the appropriate card association.
5. The card association identifies which issuing bank maintains the card and sends the authorization request to that institution.
6. The issuing bank approves or declines the transaction (based on available balance) and sends the response back to the card association.
7. The card association sends the response back to your processor.
8. Your processor routes the transaction back to your point-of-sale (POS) or property management system (PMS).
9. Your clerk receives an approved, declined, or referral response.
    - **Approved** – If you received an "approved" response, this indicates that the card has enough funds to cover the purchase, and the transaction has been authorized.
    - **Declined** – If you receive a "declined" response, the card balance cannot cover the purchase and an alternate payment method must be requested. NOTE: Do not attempt another authorization on that card for at least 24 hours. The customer may plead for you to do so, but requesting an authorization a second time may flag your account for suspicious activity. After a true decline is received, it will not change at the issuing bank until the next day. If the customer insists on running their card again, offer to call the issuing bank by phone (calling about an authorization will not flag your account).
    - **Referral** – If you receive a "voice authorization required" or "referral" response, call the voice center to retrieve a verbal authorization. (If you're ever tempted to make up an authorization code, please read our best practices section first to learn why that's a terrible idea.)

SETTLEMENT:

At the close of business or prior to opening the following day, you should submit all of your authorized transactions. This group of transactions is typically referred to as a batch.

Here's an example of how a settlement is conducted:

1. You package the transactions into a batch and electronically submit the batch to the processor.
2. The processor electronically sends the batch to your merchant bank.
3. The merchant bank issues you a credit for the amount of the batch.
4. The merchant bank groups the transactions by card brand and then sends the transactions to the corresponding card associations.
5. The card associations send your merchant bank payment for the batch of transactions.
6. The card association then identifies the issuing bank for each transaction, routes these settled transactions to the respective issuing banks, and then receives payment from the issuing bank.
7. The issuing bank then posts the transaction to the cardholder's account and sends the cardholder a monthly statement reflecting the transaction and requesting payment.
8. The cardholder receives their statement and sends back a payment to the issuing bank.

OK, so you can successfully complete a transaction and sell your goods or services to a credit card holder. But do you have the correct merchant account for your business? Read on to find out.

MERCHANT ACCOUNT

You cannot accept credit card transactions without a merchant account, and using someone else's account can get you into a world of trouble. With that in mind, let's take a look at just what's included in this account, and what it does for you.

WHY DO I NEED ONE:

You can't accept credit card transactions without it. Using another business' merchant account to accept credit cards is called "factoring" or money laundering, which is a serious violation of Visa and MasterCard rules – and a felony.

Application Fee Most merchant services providers (MSPs) and independent sales organizations (ISOs) will request an application fee from a merchant to set up a new merchant account. This is usually between $25 and $50, but could be higher. This fee is commonly waived if the merchant requests it (so be sure to ask).

Policy Changes Financial institutions commonly change policies on their accounts, which include merchant accounts. There are many reasons for these changes but most follow a merger, or when two companies blend their policies. These mergers will often redirect the focus of the financial institution. If your merchant account type is no longer of value to that financial institution, your account may be terminated. Usually, these policies are planned ahead of time and merchants are made aware of their need to find a new MSP/ ISO.

Merchant Identification When your transactions are settled and received at the issuing bank, certain identifying information is passed along with the charge. The merchant identification (MID) information populates your business name (or a portion of it) on your customer's credit card statement. If the information provided to the customer is not easily recognizable, they may file a dispute with their issuing bank claiming they never charged anything at this unknown business. The more complete and accurate information you provide during account setup, the less likely you are to see this kind of chargeback.

Types of Merchant Accounts Part of the merchant account process is choosing the right account type to match the type of business you run. Make sure that your MID is classified in the correct category for your business type. Not having the appropriate classification can mean serious downgrades on all of your transactions.

Retail This is the most common form of merchant account. Retail merchant accounts are used for businesses that provide goods and services in a face-to-face environment. If a merchant will be relying on magnetic stripe data and doesn't fall into any of the other card-present categories, this is the type of account normally used.

Restaurant Restaurant merchants follow all of the same rules and requirements as retail merchants. However, "tip" and "clerk" are two additional fields that are required by the card associations in order for a transaction to be eligible for the quoted discount rate for a restaurant.

Hospitality Hospitality merchants have more information to handle than any other merchant type. Things like check-in date, number of nights stayed, incremental authorizations, etc., make it difficult (but not impossible) for hospitality merchants to qualify for their quoted discount rate.
In the case of resorts and large, full-service hotels, it's not uncommon for there to be multiple merchant accounts of varying types on the same property.

Mail Order / Telephone Order (MO/TO):

MO/TO is used when the merchant's primary mode of sales is not conducted face-to-face with the cardholder.

There is a higher risk of fraudulent activities, and, as a result, MO/TO accounts carry higher discount rates than the previously mentioned account types. Additional security checks must be handled as well, such as Address Verification System (AVS) and Cardholder Verification Value (CVV2).

e-Commerce / Auto Rental:

e-Commerce e-Commerce merchant accounts carry the highest quoted discount rates. There are two different types of e-commerce accounts: physical and digital. A physical account represents a Web merchant that is shipping or providing some form of tangible product to the cardholder, whereas a digital merchant provides a service.

Auto Rental Auto rental merchant accounts are used solely by organizations that rent vehicles. Auto rental merchants must provide a variety of additional information specific to the auto rental agreement along with their transaction data. The majority of these transactions will be carried out face-to-face and a card swipe will occur.

While most of this section covered information you likely already know, understanding each piece of the process can help you make better-informed decisions about your payment processing setup and help you avoid costly mistakes. The next section goes into detail on the true costs of credit card processing and breaks down the too-often-hidden fees incorporated in your merchant account.

FEES:

Exactly how much money does each credit card transaction cost you? Unfortunately, there is no easy answer to that question. The various fees that can be imposed on a merchant are all too often hidden in the fine print of rules and regulations created by the card associations. Here are a few you should watch for:

Interchange Fees:

Interchange fees are the fees that card associations charge for processing each transaction. There are a variety of interchange fees that are based on how the transaction is sent and the type of merchant account. They are usually stated as a percentage of the total bill, plus a flat, per-transaction rate. Interchange fees cover the costs and time associated with getting funds to the merchant bank and getting the billing information to the issuing bank. Interchange is paid by the merchant bank to the issuing bank, which then pays the card association. Interchange fees are normally hidden from merchants. A simple Internet search for Visa interchange fees or MasterCard interchange fees will help you see how much you are actually paying.

Here's an example of the fees associated with a typical Visa retail transaction and how these fees are distributed to the various parties involved. Let's assume a discount rate for this example of 2.05% + $0.15 transaction fee.

For a $100 Visa charge, the merchant would pay their merchant services provider (MSP) $2.20. This $2.20 is paid out as follows: Visa and the issuing bank split the interchange rate of 1.65% + $0.10, or $1.75 – the MSP and processor split the .40% + $0.05 mark-up, or $0.45.

Because there are dozens of different rates and fees that can be assessed to the merchant, some processors and MSPs choose to bundle these various rates together into "rate tiers." Rate tiers are usually more simplistic than interchange fees in their naming, such as "qualified," "mid-qualified," and "non-qualified." While this may seem simpler to understand, it actually makes it more difficult for a merchant to understand what they are actually paying for and why.

It should be noted that only Visa and MasterCard actually partake in the interchange process. Other cards such as American Express and Discover do not participate in interchange. Cards like these act as their own issuing bank, merchant bank, and card association, handling all aspects of the card transaction and not sharing any of their fees.

Discount Rate vs. Effective Rate:

Ever wonder why your monthly MSP/independent sales organization (ISO) bill is more than what you were quoted? That's the difference between the discount rate and the effective rate. The discount rate is the fee you would pay to your MSP or ISO to handle the deposit of credit card funds into your merchant account if everything ran perfectly. It was negotiated at the time you selected your MSP and is usually quoted as a percentage or fraction of your transaction volume (also known as basis points). The discount rate is the amount your deposit will be discounted (e.g., a $10,000 deposit with a discount rate of 2.03% would become $9,797).

Remember when we said the discount rate applies when everything runs perfectly? Well, in reality, we all know that never happens; as a result, your effective rate is the true cost of each transaction, which can really add up. You can figure the effective rate by adding together all of the fees and charges that were assessed to you and dividing those by the total dollar amount that you processed. But when you understand

what each line item fee actually is on your bill, you can then make smarter choices and keep your MSP from overcharging you.

Authorization Fee / Communication Cost:

Authorization Fee All processors charge a flat fee per transaction for the authorization request. This fee may be listed as its own line item on your statement or it may be "bundled" into your discount rate. Some MSPs will state they are waiving this fee, but usually it is just being "bundled" into your discount rate.

Communication Cost Your communication cost is what you pay to move a transaction from one point to another. This cost varies greatly depending on your chosen method of connection. A dial-up connection is still often used but can be costly, since the processor has to maintain toll-free phone circuits and modems for the calls into its network. Another option is using an Internet connection. This option can be fairly inexpensive to the processor and therefore should be cheaper for you. However, some processors see this as a "premium" due to the speed you enjoy by using these connections, so they add a "premium fee."

Another form of communication is a private line between the merchant and the processor. With this type of connection, the merchant is charged a monthly support and maintenance fee for the dedicated line. Private lines are primarily used by very large merchants that process thousands of transactions per day and, since the merchant has a separate agreement for this line, there are no communication costs in the discount rate. This is a fairly expensive option and only recommended for very large merchants.

The most cost-effective communication option is for merchants to take advantage of a gateway, such as Jackrabbit, which uses its own dedicated connection to the merchant's processor and therefore merchants can save considerable money since the gateway pays to connect to the processor.

MSPs often bury communication costs into their rates in order to pass them on to their merchants. They may also appear on the customer's statement as 950, 800, or wide-area telephone service (WATS) fees. If you aren't seeing communication costs on your statement, they are likely being "bundled" in the discount rate. Jackrabbit does not pass any communications costs on to the merchant – "bundled" or otherwise.

Downgrades / Credits:

Downgrades A large portion of the costs associated with credit card acceptance is the downgrading (non-qualification) of transactions. These are the transactions that do not qualify for the best possible discount rate because they don't meet the data content or transaction timing regulations set by the card associations.

When a transaction is downgraded, the merchant is charged additional basis points on top of the quoted discount rate. The exact amount is dependent on the type of error that occurred with the transaction.

There are many reasons for a transaction to be downgraded. A few of the most common are: failure to settle within two days of initial authorization, missing/invalid transaction ID or Banknet data, missing or corrupt swipe data from the magnetic stripe read of the card, or no AVS attempt on manually keyed transactions.
Credits Many merchants don't realize how much issuing credits can cost them. While most MSPs charge nothing for issuing credits (aside from a communication fee), you have to keep in mind that you already paid for the transaction you are now trying to correct.

For example, what if you key in a transaction for $15, but accidentally add an extra zero, making the transaction $150? Assuming the discount rate is 2%, the cost to process this $150 transaction is $3. After issuing the credit, you end up having paid $3 in fees on a $15 charge – that's essentially a 20% effective rate.

American Express & Discover:

Accepting card brands such as American Express and Discover can be an expensive endeavor for merchants. However, with nearly 40% of all business travelers utilizing American Express as their corporate credit card and millions of cardholders carrying Discover cards, it's viewed as a necessary expense.

These cards typically add to your costs because they require you to pay a third-party routing fee just to connect to their processors. This fee can be as high as $0.25 per authorization. While your MSP may tell you that they don't charge for American Express or Discover transactions, this is almost never the case. The cost may be buried in the discount rate, but since third-party processors charge the MSP, you can be assured the charges are passed on to you somehow. Jackrabbit provides our direct connections to First Data at no cost to the merchant.

Chargebacks / Additional Charges:

Another type of charge you may see is a chargeback. On any given credit card transaction, the cardholder has up to 60 days from the time he receives the statement referencing the transaction to dispute the charge. When the cardholder files a complaint with his issuing bank that a charge was not valid, the issuing bank generates a retrieval request that is sent to the merchant. To respond to a retrieval request, merchants are charged a fee by their MSP. This fee runs from $10 to $50 per retrieval request (the average is $15). With Jackrabbit's two-year transaction archive at your fingertips, you will never have to pay another retrieval request fee.

If the merchant does not respond in a timely manner, a timeliness fee can also be charged and you may even lose the transaction completely. There are a variety of other instances that may result in a chargeback that do not require the cardholder to initiate the event. These are initiated by the processor, merchant bank, or issuing bank. Even a partial reversal of the original amount of the transaction is considered a chargeback.

In addition to the fees directly tied to processing the transaction, you should also be aware of statement fees, monthly minimums, annual fees, voice authorization fees, termination fees, and application fees. These are common fees that need to be considered as part of the cost of processing transactions.

Unfortunately, there is no hard rule regarding these additional charges. For some, the decision to charge (or how much to charge) is made on a merchant-by-merchant basis. Because there can be such a variance in these fees, it's wise to shop around and compare rates/quotes from several MSPs to ensure you're getting the best rate possible for your business.

SECURITY:

Card brands and industry organizations, like those behind the Payment Card Industry Security Standards Council (PCI SSC), are constantly modifying their security requirements as a result of persistent and ever-increasing threats from hackers and thieves. However, simply complying with industry regulations at audit time is not enough to counter these threats. As a merchant, security must be part of your daily routine in order to protect yourself and your customers from experiencing costly fraud and breaches.

The Payment Card Industry Data Security Standard:

In December 2004, the card associations came together to standardize the handling of credit card security. The Payment Card Industry Data Security Standard (PCI DSS) was the result of their efforts. PCI DSS is based on six practices:

- Building and maintaining a secure network
- Protecting cardholder data

- Maintaining a vulnerability management program
- Implementing strong access control measures
- Regularly monitoring and testing networks
- Maintaining an information security policy

Keeping current with PCI DSS is a must; failure to comply with the procedures and standards of PCI DSS can result in fines, financial and operational penalties, and even the loss of your merchant account.

Payment Application Data Security Standard:

The PCI SSC introduced the Payment Application Data Security Standards (PA DSS) in 2008. PA-DSS is a comprehensive set of payment application security requirements. Vendors who develop and sell payment applications to merchants must have their products PA DSS-validated by a Payment Application Qualified Security Assessor (PA-QSA). Merchants who purchase and properly implement PA DSS-validated payment applications as part of their overall data security program can be assured that cardholder data is not retained or stored post-authorization.

It's important to note that merchants who are using payment applications that are not PA-DSS-validated will never be compliant with PCI DSS.

Summary of Laws & Regulations:

There are a variety of federal and state laws that govern credit cards and transactions. A collection of these laws can be found at the FTC's credit website, www.consumer.ftc.gov. Be sure to review the Fair Credit Billing Act found on that page.

Now you are familiar with the compliance requirements of PCI as well as the laws and regulations that govern or edit cards and transactions. You may also understand that meeting these standards is not enough to give you foolproof protection from thieves and skilled cyber criminals. In the next section, we will take a deeper look at the many different types of fraud and what you can do to make security a part of your daily routine.

FRAUD:

As a consumer and cardholder, you have surely heard the stories of identity theft and credit card fraud that have showered the news. As a merchant, this news takes a whole new level of importance; you need to be well-educated on the common types of fraud and how to counteract fraud in your organization.

Economic Impact / "Trusted-Employee" Fraud:

Economic Impact Each year, billions of dollars are lost to credit card fraudsters and identity thieves. These crooks are sophisticated and operate in organized, multinational groups rather than as individuals. While these attacks can result in huge financial losses for the merchant, it's often the negative publicity that does the most harm. Creating distrust between the merchant and their customers can, in some cases, put the merchant out of business.

"Trusted-Employee" Fraud "Trusted-employee" fraud is rapidly becoming one of the most common (and costly) forms of fraud affecting business today. "Trusted-employee" fraud is typically the result of disgruntled employees issuing credits to their own credit cards (or those of their friends) through your merchant account. Another tactic these thieves employ is to void transactions after a sale to put money in

their pocket from the register or to provide free goods or services to friends. Even more frightening are the cases involving criminals or groups of criminals who gain employment with the sole intent of committing fraud.

Skimming / Phishing:

Skimming Easily configurable "skimming" devices allow an individual to swipe a credit card without a standard terminal. Once swiped, the thief has all of the magnetic track information for the card and can easily create a new card based on that track information or use the card number contained in the track information for transactions over the Internet. Skimming devices allow a thief to swipe and maintain thousands of card numbers. These fraudsters then use your customers' credit card information to make fraudulent purchases on the Internet or sell the card information to other criminals.

Phishing Probably the most difficult method of fraud to detect, phishing involves criminals setting up a website and creating emails that look like legitimate emails from established companies. In most cases, these spoof shops have no intention of running a transaction; they just collect a cardholder's information and card number. They store this information and use it for their own purchases – quickly selling anything they buy so they can pocket the cash. Some of these shops share the cardholder's information with other fraudsters.

Bank Fraud / Cardholder Fraud:

Bank Fraud The employees of banks, processors, and merchant services providers (MSPs) have access to thousands of card numbers. They may use this information for themselves or sell it to criminals. They may even create fake merchant accounts, cardholder accounts, or credit cards.

Cardholder Fraud Cardholder fraud is extremely difficult to identify and prevent. It occurs when a legitimate cardholder purchases goods or services and then files a dispute claiming that they never received the goods or services for the transaction. They may even report the card as stolen immediately after making the purchase. Other cases involve friends or family of the cardholder "borrowing" the card without permission to make a purchase and then returning it to the cardholder without them knowing it left their possession.

Number Generators / Stolen, Altered, & Fake Cards:

Number Generators These are software applications that provide thieves with thousands of potential card numbers. Once the thief has these numbers, they simply have to figure out which ones are active. This is done with simple software that will run a small dollar transaction with each of the cards. When an approval is received, the thief knows they have a "real" card and can use it to make large purchases on the Internet.

Stolen, Altered, & Fake Cards Once a card is in the possession of thieves, they will use it as quickly as they can to make as many purchases as possible before the card is reported stolen.

An altered card has physical parts of it modified. This could be anything from changing the expiration date, signature panel, or even re-encoding the magnetic stripe with another card number.

Fake cards are harder to identify than counterfeit currency. Criminals can produce legitimate-looking cards and then emboss and encode the card with a stolen credit card's information.

Identity Theft / Hackers / International:

Identity Theft Once an individual's identifying information has been compromised, a thief can use it to set up new accounts in that person's name or they can take over an existing account of that person. Whether it is a merchant's dumpster or the cardholder's own curbside trash, thieves will dig through garbage bins to

look for any information that may have been discarded that they can use. Credit card numbers, social security numbers, address information, and birth dates mean big money to a thief and bigger headaches for the individual whose information is stolen.

Another simple tactic employed by thieves is to covertly watch people in the checkout line or at the ATM. Driver's licenses, ID cards, checkbooks, and credit cards are often exposed in wallets and purses as their owners make purchases. All a thief has to do is snap a quick picture with their cell phone and your information is theirs. Once this information is acquired – whether by rummaging through garbage or looking over a person's shoulder – there is nothing to stop the thief from making purchases or setting up new accounts in the victim's name.

Hackers When hackers find a way into a merchant's website, POS, or PMS, the system is theirs. Hackers use viruses against their victims' computers, which turns these infected computers into fraud machines that send out malicious software to infect more systems. Recent headline-making data breaches have shown us that these threats are increasing.

International The vast majority of credit card fraud perpetrated against Americans is committed overseas. Many e-commerce merchants will not even conduct business with foreign-issued credit cards. There are criminal organizations in some countries that have ties to their local banks and therefore access to illicit information that can then be used to do fraudulent business with U.S. merchants via the Internet.

Things to Watch for:

Want to Prevent Fraud at Your Business? Here Are a Few Things to Watch for:

- Customers who make major purchases without asking any questions should raise a red flag. You know what your typical customer is like; if someone is buying the most expensive item in your store without asking you the kinds of questions you would normally receive about that item, you may have a problem.
- Customers who purchase a large quantity of merchandise and you feel like something is out of place or suspicious. Either a variety of items, different sizes of the same thing, or similar items with big price differences can indicate something is off with a purchase. If it looks like the customer didn't put a lot of thought into his shopping, chances are he didn't. Be vigilant.
- Customers who are pushy or rushing through the checkout process. They may be trying to throw the clerk off guard before slipping them a fake or stolen card. Make sure that your staff knows to take their time when going through the transaction process.
- Customers who make a purchase, leave the store, and then return shortly afterward for another, larger purchase. The first may have been a test run before the big take.
- Customers making high-dollar purchases at these unusual times. Thieves attempt to make fraudulent purchases when businesses open in the morning or just before closing, when clerks have many things to do and may be too busy to notice a suspicious transaction.
- Customers who are insistent about you not knowing where they live. Be wary of a customer who declines free delivery on a large item and scrutinize the transaction even further.

We hope you have found the information in our Credit Card 101 tutorial to be useful. Please feel free to share it with a colleague by using the links below. To learn some best practices for processing payments in your business, read the next section.

BEST PRACTICES:

It used to be that your merchant bank or merchant services provider (MSP) worked as your advocate; they would help merchants like yourself navigate the confusing world of payment processing. Sadly, today this is becoming less and less common. Now they profit from your mistakes and have no incentive to help you avoid them.

In the spirit of merchant advocacy, here is a list of best practices (based on decades of industry experience) designed to get you on the right track and help you avoid the most common pitfalls.

Setup / Education:

Setup

1. Make sure you've identified the correct merchant type for your business.
2. If you have more than one merchant type (e.g., spa, hotel, restaurant), set up each location and merchant ID (MID) separately.
3. Make sure your processing setup provides the ability to process transactions directly to American Express (AMEX) if they account for more than 25% of your transactions.
4. Publish a refund policy so your customers know the steps they must take to return merchandise or receive reimbursement for services. Place your policy around your cash registers, near the signature line of the receipt, and on your website.

Education Well-trained employees are your first line of defense against credit card fraud. We recommend you make every effort to provide thorough training for your staff to detect and stop fraud. The following are some items you might include in your training:

- Make sure employees know to check the physical appearance of the card for any alteration, expiration dates, and the cardholder signature.
- Establish that employees compare the name on the card with the identification of the person presenting it in card-present transactions.
- Ensure that each of your employees creates their own unique password and logs off when not at the register.
- Establish reliable end-of-day auditing procedures for all staff. All employees should be thoroughly trained on your point-of-sale (POS) or property management system (PMS) tools.
- Assure employee familiarity with the differing requirements for accepting and processing Visa, MasterCard, American Express, and Discover. Acquire the latest published handbooks to keep your employees up-to-date on card brand changes.

AVS & CVV2:

Address verification service (AVS) is a simple check that compares information presented by the cardholder with billing information on the account for the card. The cardholder verification value (CVV2) check is a three- or four-digit number that is printed on the physical card and is stored only by the issuing bank for that card. The merchant should always run AVS and CVV2 checks for card-not-present transactions.

AVS Each issuing bank supports different levels of verification. The most widely accepted and supported form of verification is the ZIP code. If the cardholder cannot identify the billing ZIP code for that card, you should further scrutinize the transaction. Each AVS authorization request sent to the issuing bank will return back two separate responses; one response tells whether the dollar value of the transaction is approved and the other tells whether the AVS information supplied for verification matched the information on file for that cardholder. Your software should be configurable to decline transactions based on declined AVS responses if that is the business practice you wish to adopt.

CVV2 The CVV2 process is similar to AVS. The CVV2 value is passed to the issuing bank along with the authorization request. The issuing bank will reply with two responses; one response authorizing the dollar amount and a second identifying whether the CVV2 provided matched the card. If you don't get a CVV2 match during authorization, you may not want to accept that card for payment. Your POS/PMS should be configured to decline transactions based on declined CVV2 responses if that is the business practice you wish to adopt.

CVV2 can also be referred to as the CID or CVC2. Never record the CVV2 for any reason, as doing so may compromise the card's security.

Auditing Transactions / Settling Batches:

Auditing Transactions Balancing your daily batches with your POS/PMS before settlement is a powerful way to minimize your effective rate. If errors are discovered after settlement, merchants may pay fees for a transaction for which they will ultimately not receive funding. Timely adjustments made before settlement can save you a lot of money.

Most POS/PMS provide a daily totals report with a sum of all credit card transactions processed. They may even provide a list of the individual transactions that are included in that sum. This total should be compared to your credit card batch to ensure that what you are submitting for funding exactly matches what your sales for the day were in your POS/PMS. Be sure that your credit card solution has tools that enable you to rectify any discrepancies in your reports (prior to batch settlement) in order to eliminate duplicates, prevent chargebacks, and reduce your fees.

Settling Batches Settle your batches daily. This will help ensure that you're getting the best rate possible on your transactions. Transactions not settled within 24 hours are considered high-risk. They may not qualify under your contracted rate and have a higher likelihood of being disputed by the cardholder.

Contact your MSP and verify the cutoff time for funding of settled batches. This will help you prioritize your batch settlements and ensure funds are more rapidly deposited into your account.

Debit Cards:

Debit cards let buyers pay for goods and services with funds from their checking account and are an important part of any merchant's business. Debit cards give consumers more flexibility in their payment options and can be used in two ways: online debit and offline debit.

- **Online Debit** – Sometimes referred to as PIN debit, online debit is processed on the debit network of the cardholder's bank. The card is swiped or inserted at the POS and the customer is asked to enter their personal identification number (PIN). As a merchant, you must be specifically set up to accept these types of transactions through your merchant account and you must have a keypad to accept the PIN entry from the customer.
- **Offline Debit** – Sometimes referred to as signature debit, offline debit is processed in a manner similar to a credit card transaction. If the debit card carries a card brand, such as Visa or MasterCard, the card may be processed by simply swiping it through a credit card terminal that supports that card's brand. The transaction is processed over the merchant's credit card network and the customer provides their signature as approval of the transaction.

Merchants need to be aware of the fees associated with both forms of debit transactions. Offline debit transactions are processed through the card association interchange, which requires the merchant to pay an interchange fee. With an online debit transaction, the transaction is processed through the debit network, typically for a flat, per-transaction fee.

System Down and Voice Authorization:

System Downtime and Voice Authorization Brief periods of downtime with your online payment services are inevitable; voice authorization may be needed to complete a transaction when connection problems occur. Therefore keep the phone numbers of the card issuers you accept handy. (Don't trust the number on the back of the card, as they are often modified by fraudsters.) The voice authorization obtained should be recorded and notated on the sales receipt. Many merchants also keep knuckle-busters (manual credit card imprinters) and authorization slips handy for when connection problems occur.

False Authorization Codes Creating false authorization codes is not recommended under any circumstance. Your staff may, when rushed by many customers at once, desire to expedite the checkout process by creating false codes.

Under current credit card regulations, a merchant forfeits all chargeback defenses when false authorization codes are used. While some processors will process false authorization codes and then fine you, other processors, when they receive fake authorization codes, disregard them and don't process the transactions at all. The card associations – Visa, MasterCard, American Express, etc. – have stated that fake authorization codes will incur a fine, possibly up to $50 per incident! Have your staff make calls to your authorization center in order to obtain valid credit card authorizations – even if that means taking a few extra seconds to do so.

Chargebacks:

Chargebacks occur when a consumer disputes a credit card charge. The credit card company withdraws the money for a transaction from a merchant's account and gives it back to the customer. Cardholders have 60 days from the date they receive their statement to dispute a charge, and the issuing bank has 120 days or more after the transaction date to file a dispute with the merchant.

The process begins with a retrieval request to the merchant. If you receive a retrieval request, be sure to respond to it as quickly as possible. Failing to respond will result in the transaction being charged back and you'll not only lose the funds from that transaction, but the status of your merchant account may be put in jeopardy. Each card brand has its own complex guidelines regarding merchant chargebacks which, if not handled correctly, can result in arbitration. Be aware: each retrieval request will cost you money.

Common Merchant Mistakes:

Following these guidelines will help you avoid fines and/or the loss of your merchant account:

1. Never run your personal credit card through your merchant account.
2. Don't process transactions through your merchant account to provide cash for yourself or others.
3. Examine all cards closely. An expired card that gets a valid authorization from the processor will not return a payment to the merchant.
4. Don't allow the use of your merchant account by another merchant. This is called "factoring" and it can lead to the loss of your merchant account and liability for any criminal activity that was being handled in those transactions. Also, any disputes or chargebacks filed go against your merchant account.
5. Do not impose a maximum on transaction amounts. Currently, you may restrict transaction amounts to a minimum up to $10, provided that you don't discriminate between card types charged.
6. Don't split up a transaction into smaller transactions. Not only can this get you in trouble with your MSP, but the customer may only claim one of the charges and not all of them, resulting in a chargeback.
7. Do not request a credit card to guarantee a check.
8. Keep your MSP aware of changes and growth in your business. If you have a merchant account for your brick-and-mortar locations and decide to branch out to the Internet, you'll need an additional merchant account to handle online payment transactions. Processing Internet transactions with your brick-and-mortar merchant account can lead to serious fines or even the loss of your merchant account.
9. Do not print complete card numbers on your receipts. Common practice is to print only the last four digits of the card number on the receipt.
10. Get an authorization for every credit card transaction you settle.
11. Take every measure possible to prevent duplicate transactions. Duplicate transactions will nearly always result in a credit, dispute, or chargeback, which means fines and – if it happens too often – the loss of your merchant account.

12. Read and understand your merchant agreement before signing it. The agreement outlines the various fees, charges, rules, and regulations you need to be aware of. If there is any portion of the agreement that you don't understand, have your MSP give you a written explanation of it. After you have signed the merchant agreement, you are committed to the rules within it.
13. Make resolving customer issues a priority. If you refuse to help a customer resolve a credit card charge, they may take the problem to their issuing bank. Excessive disputes can and will have negative repercussions on your merchant account.
14. Take advantage of the variety of fraud screening products and services available to merchants before a theft occurs; you might not be able to do anything about it after something happens.
15. When investigating a business venture or business partner, examine their credit history.
16. Be certain that old merchant accounts are properly terminated. When getting rid of terminals and other credit-card-related equipment, make sure that proper steps have been taken to close the equipment out of all transactions to make sure you get funded for your sales. Contact your processor's support center to find out how to clear the memory of the equipment. Some processors might attempt to charge you non-compliance fees after you have closed your account with them. Check with your processor to know if and when they charge PCI fees.
17. If your business is going to experience uncommonly high sales volume (e.g., triple the normal monthly sales volume), notify your MSP. Uncommonly high sales volume can raise flags and mark your business as a potential financial risk. Failure to do so may result in a cessation of services, a withholding of all or some of your funds in "reserve" to help cover the potential financial risk, or outright termination of your account. Furthermore, it may be several months before those funds are released to you if your MSP is investigating the variance in monthly sales volume.