UniBul
MERCHANT SERVICES

Card Acceptance Best Practices for Lowest Processing Costs

I. **Card Acceptance Best Practices Goal.** The credit card companies and associations require that their cards are accepted according to a set of rules that each one of them publishes at least once per year. At UniBul Merchant Services we help you understand what these rules are and implement them into your sales process to ensure that you:

a. **Get the lowest possible processing rates.**

b. **Minimize fraudulent transactions.**

c. **Reduce chargebacks.**

II. **Website Requirements.** Certain content or features should be clearly displayed on your website. These elements are intended to promote ease of use for your customers and reduce potential disputes and chargebacks.

a. **Customer service contact information.** Customer service telephone number as well as email address should be clearly displayed on every page of the website, on shipping materials and on monthly statements. If customers cannot contact you when they have a question, they will contact their card issuer which may result in a chargeback.

b. **Policies.** Return, refund, cancellation and delivery policies should be available to online customers through clearly visible links on your home page. You should also provide “click-through” confirmation for important elements of the policies to require customers to click on an “Accept” or “Agree” button to acknowledge that they understand and accept these policies.

c. **Order and refund confirmations.** Send email confirmations and summaries within one business day of processing orders and refunds. State time frames for refunds and indicate that a full billing cycle may be needed for the card issuer to apply the credit to the cardholder’s account.

III. **Transaction Processing.** The credit card companies and associations have established a range of fraud-prevention policies, guidelines and services. Implementing these tools and best practices will help protect you from fraudulent transactions and will reduce chargebacks.

a. **Cardholder information.** Get the cardholder’s name and address. If the shipping address differs from the billing address, follow-up with a phone call or an email to verify the order. Be sure to ask for a phone number in your order form.

b. **Card information.** Get the card number and type (most consumers don’t know that a card’s type can be determined by the card number), the card’s expiration date (make sure it is in the future) and the Card Verification Code - the 3-digit number, located on the back of each card (or the 4-digit number on the front for American Express cards). The Card Verification Code serves to ensure that the customer is in physical possession of the card.

c. **Implement Verified by Visa and MasterCard SecureCode.** Visa and MasterCard introduced these tools to help merchants fight fraud and reward merchants who use them with very strong representment rights in cases of chargebacks (more details about these two programs in Chapter XIV - Credit Card Authentication).

d. **Always use AVS.** The Address Verification Service (AVS) allows you to verify a cardholder’s billing address by comparing it to the one on file with the card issuer. The perpetrators of fraud often do not know the account’s correct billing address (more details in Chapter XII - Address Verification Service).

e. **Only ship to an AVS verified address.**

f. **Deliver the merchandise or services to the cardholder at the time of the transaction.** If that is impossible, inform the cardholder of the delivery method and the tentative delivery date. Transactions must not be deposited until goods or services have been shipped.

g. **Do not use voice authorizations.** They bypass the processing bank's systems and cannot be used as supporting evidence in chargeback representments. Do not force authorizations which happens when you key-enter voice-authorized transactions.

h. **Each deposit should refer to one authorization.**

i. **Ship within seven days of authorization.** Otherwise you should obtain a new authorization.

j. **Deposit transaction receipts within three days of the transaction date.** For card-not-present transactions, the transaction date is the shipping date, not the order date. Transactions deposited more than 30 days after the original transaction date may be charged back to you.

k. **Use the same transaction ID returned from your authorizations for your deposit and refund transactions.** This eliminates deposits of refunds where authorizations have not been performed and can substantially reduce fraud.

IV. **Payment Card Industry (PCI) Data Security Standard (DSS).** In 2006 all major credit card companies joined forces to create the Payment Card Industry Data Security Standard to address the growing problem of data security compromises in the payment card industry. All merchants must comply with this standard and periodically review their compliance. Failing to do so can result in significant fines and, potentially, in cancellation of their merchant accounts.

a. **PCI DSS requirements.** The following 12 requirements comprise the PCI DSS requirements:

i. **Install and maintain a firewall configuration to protect cardholder data.** All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' internet-based access through desktop browsers, or employees' email access.

ii. **Do not use vendor-supplied defaults for system passwords and other security parameters.** These passwords and settings are well known in hacker communities and easily determined via public information.

iii. **Protect stored cardholder data.** Encryption is a critical component of cardholder data protection. Also, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full personal account number is not needed and not sending it in unencrypted e-mails.

iv. **Encrypt transmission of cardholder data across open, public networks.**

v. **Use and regularly update anti-virus software or programs.** Anti-virus software must be used and regularly updated on all systems commonly affected by viruses to protect systems from malicious software.

vi. **Develop and maintain secure systems and applications.** Many security vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches.

vii. **Restrict access to cardholder data by business need-to-know.**

viii. **Assign a unique ID to each person with computer access.** This requirement ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

ix. **Restrict physical access to cardholder data.**

x. **Track and monitor all access to network resources and cardholder data.** Determining the cause of a compromise is very difficult without system activity logs.

xi. **Regularly test security systems and processes.**

xii. **Maintain a policy that addresses information security for employees and contractors.** All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

b. **Data storage.** The following table shows what data can and cannot be stored:

Data Type	Data Element	Storage Permitted	Protection Required
Cardholder data	Primary account number (PAN)	Yes	Yes
	Cardholder name*	Yes	Yes
	Service code*	Yes	Yes
	Expiration date*	Yes	Yes
Sensitive authentication data**	Full magnetic stripe	No	n / a
	Card Verification Code	No	n / a
	PIN / PIN block	No	n / a

* These data elements must be protected if stored in conjunction with the PAN. This protection must be consistent with PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of these data or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

**Sensitive authentication data must not be stored subsequent to authorization (even if encrypted).

c. **Merchant level definitions for PCI certification.**

Merchant Level	Definition
Level 1	Level 1 are merchants processing over 6 million Visa or MasterCard transactions per year.
Level 2	Level 2 are merchants processing from 150,000 to 6 million Visa or MasterCard transactions per year.
Level 3	Level 3 are merchants processing from 20,000 to 150,000 Visa or MasterCard transactions per year.
Level 4	Level 4 are all merchants not included in Levels 1, 2 or 3.

d. **PCI certification requirements by merchant level.**

Merchant Level	Annual On-Site Review	Annual Self-Assessment	Protection Required
Level 1	Required by a certified 3rd party	n / a	Required by a certified 3rd party for external IP addresses.*
Level 2	n / a	Required to complete questionnaire.**	Required by a certified 3rd party for external IP addresses.*
Level 3	n / a	Required to complete questionnaire.**	Required by a certified 3rd party for external IP addresses.*
Level 4	n / a	Recommended annually.	Recommended annually.

*Internet accessible.
**PCI self-assessment questionnaire.

V. Chargebacks.

a. **What is a chargeback?** A chargeback is a transaction that a card issuer returns to a merchant's processing bank - and most often to the merchant - as a financial liability. In essence, it reverses a sale and the merchant's account is charged for the amount of the transaction.

b. **Chargeback reasons.** The most common reasons for chargebacks are:

   i. **Customer dispute.** A customer may dispute a transaction because a credit was not issued when the customer expected it to be; merchandise was not received; a service was not performed as expected; the purchase was fraudulent.

   ii. **Fraud.**

   iii. **Processing errors.**

   iv. **Improper authorization.**

   v. **Inaccurate transaction information.** Many chargebacks result from easily avoidable mistakes, so the more you know about proper transaction processing procedures, the less likely you will be to inadvertently do, or fail to do, something that might result in a chargeback.

c. **Your responsibility.** You have a direct responsibility for taking action to remedy and prevent chargebacks. In most cases, the full extent of your financial and administrative liability for chargebacks is spelled out in your merchant agreement.

d. **Chargeback remedies.** Even when you do receive a chargeback, you may still be able to resolve it without losing the sale. Simply provide your processing bank with additional information about the transaction or the actions you have taken related to it.

VI. Avoiding chargebacks.

Most chargebacks result from inadequate payment processing procedures and can be prevented with appropriate training. The following best practices will help you minimize chargebacks:

a. **Always conduct an AVS check and ensure that you received a "positive AVS,"** i.e. Address + 5 ZIP or Address + 9 ZIP. Only ship to a billing address with an approved AVS response.

b. **Obtain evidence of receipt** of goods (e.g. signed shipping receipt).

c. **Use Verified by Visa and MasterCard SecureCode** (for eCommerce only), which guarantees the card was used legitimately by its owner and gives you strong representment rights.

d. **Always require a Card Verification Code.**

e. **Process refunds as quickly as possible** and notify consumers in writing when a refund has been issued or a membership canceled. Provide them with the date of refund and a cancellation number, if applicable.

f. **Always provide a clear billing descriptor and phone number** so the consumer can contact you directly rather than calling their bank to discuss any dispute.

g. **State terms and conditions of the sale (or membership) clearly and in plain view.**

h. **Use email to notify the consumer at each billing cycle (for recurring transactions).**

i. **Obtain a signature from the cardholder** giving you permission to charge their card on a regular basis for monthly fees or recurring payments.

j. **Make it very easy for members or subscribers to cancel -** have a "no-questions-asked" policy.

k. **Authorizations must always be "positive" and done for every deposit** and deposits must not exceed the amount you have authorized.

l. **Avoid using voice authorizations.**

m. **When an authorization is more than 7 days old, you must reauthorize the transaction.**

VII. **Processing Fees.** Understanding card transaction fees is key to keeping processing costs under control. Card processing fees are comprised of two major components:

a. **Interchange fees.** When your customer uses Visa or MasterCard to pay for a product or service, you are charged a compound transaction fee, the largest portion of which is the interchange. The interchange fee varies by card type (e.g. consumer, rewards, commercial, etc.) and payment acceptance environment (i.e. face-to-face or card-not-present). **This fee is collected by the card issuer** and consists of:

i. **A percentage of the purchase (for example 1.80%).**

ii. **A small transaction fee (for example $0.10).**

iii. **A tiny transaction percentage fee (less than 0.1**%), which goes to Visa or MasterCard and is referred to as the "Assessment".

b. **Fees charged by your payment processor.** Your processing bank charges you another fee for its services, either per transaction or bundled with the interchange and assessment. If the latter, the resulting charge is called a discount. The discount in turn can be a flat percentage, or like the interchange, it may consist of a percentage fee plus a per-item charge. If you are paying a bundled discount rate, you should seriously pursue different pricing terms, paying for the interchange and assessments on a pass-through basis (a.k.a. interchange-plus pricing).

VIII. **Pricing Models.** The most widely used pricing structures can be grouped in the following categories:

a. **Tiered pricing model.** When a merchant is charged a bundled discount, each transaction is evaluated based on pre-determined characteristics (e.g. type of card used) and placed in one of a couple of groups. These groups are as follows:

i. **Qualified transactions.**

1. **When a transaction is processed in accordance with the rules** and standards established in the Payment Processing Agreement, signed by the merchant and the processing bank, **and**

2. **It involves a regular consumer credit card**,

It is charged the most favorable discount rate. This rate is called a "Qualified Rate" and is set in the Payment Processing Agreement. The Qualified Rate is set based on the way a merchant will be accepting a majority of their credit cards. For example, for an internet merchant, the internet interchange categories will be defined as Qualified, while for a physical retailer only transactions where cards are swiped through a terminal will be Qualified.

ii. **Non-qualified transactions.**

1. **When a special kind of credit card is used (like a rewards card or a business card), or**

2. **A payment is not processed in accordance with the** rules established in the Payment Processing Agreement, **or**

3. **It does not comply with some applicable security requirements**,

The transaction is charged a discount rate that is less favorable than the Qualified. This rate is called a "Non-Qualified Rate."

iii. **There are other tiered pricing structures**, like the 3-Tier Pricing (where a Mid-Qualified category is added), and even a 6-Tier Pricing model, but the 2-Tier Pricing (Qualified and Non-Qualified) is by far the most prevalent among them.

b. **Interchange-plus pricing model.** Interchange-plus is the pricing structure where Processors add a surcharge to the interchange fee charged by the card issuers for each card transaction. This surcharge is the fee the Processor charges for providing processing services to the merchant. The fee can be a percentage of the transaction amount, a fixed per-transaction amount, or a combination of both, and remains the same for all interchange fee categories.

IX. **Tiered vs. Interchange-Plus Pricing.** With the interchange-plus pricing model each transaction is settled not at a predefined rate (as with the tiered one) but at a rate that is equal to the sum of the interchange fee set by Visa and MasterCard (and which varies by card type) and the fixed service fee that the Processor charges. Given that the interchange fees are determined by Visa and MasterCard and that neither the Processor, nor the merchant has any influence over them, the only fee that can really make a difference, is the Processor's service fee. While with the bundled discount rate the Processor's fee can vary widely for different types of cards, with the interchange-plus model for each card transaction the merchant is charged the same Processor fee. Let's use an example to illustrate the comparison.

a. **Tiered pricing.**

i. **Consumer Visa card transaction.** If an internet merchant is processing a payment according to all applicable standards, and the card being charged is of a consumer type, this will result in a Qualified Transactions and will be processed at the most advantageous rate, e.g. **2.25% + $0.25**, which is a pretty reasonable rate. In this case the interchange fee would be **1.80% + $0.10**, leaving the processor with a profit in the amount of **$0.45 + $0.15** of the transaction amount.

ii. **However, if the card was a Visa rewards card**, the transaction would be classified as a Non-Qualified Transaction and the merchant would be charged a higher rate, typically at **3.25% + $0.30**. The interchange fee for the Visa rewards card would be **1.95% + $0.10,** giving the processor a much heftier profit of **1.30% + $0.20** of the transaction amount.

b. **Interchange-plus pricing.** From the example above:

i. **A consumer Visa card transaction** would again be processed at **1.80% + $0.10** plus the Processor's surcharge. If the surcharge is **0.45% + $0.15**, the merchant will again be charged a total of **2.25% + $0.25** for the transaction.

ii. **If the card was a Visa rewards card**, the interchange fee would be **1.95% + $0.10**. The Processor's surcharge would still be **0.45% + $0.15** and the total - **2.40% + $0.25**.

c. **Comparison.** It is almost impossible to predict with absolute certainty how a particular transaction will be qualified in a tiered model. Moreover, in a tiered pricing structure the Processor needs to set the Non-Qualified rate at a level that is sufficiently high to ensure that no transaction is processed at a loss. As a consequence, and as evident in the example above, the Processor fee component of the total processing charge will vary widely from transaction to transaction. The two models start from the same point - a consumer type credit card is processed at the same rate – **2.25% + $0.25**, but then they differ significantly in the case of a rewards card: (**3.25% + $0.30) – (2.40% + $0.25) = 0.85% + $0.05 – a difference of more than 25% of the interchange-plus rate!**

X. Typical Issues with Card Processing Fees.

a. **Interchange refund.** When a merchant processes a refund, the card issuer returns the interchange to the processing bank. At this point the Processor has two options: to keep the returned fee or to pass it on to the merchant. **Make sure that the processor passes on the returned interchange to you!** The processor should keep nothing more than its own fee they charged to facilitate the transaction.

b. **Downgrades.** As shown earlier, if your pricing is based on the tiered model, your Non-Qualified transactions are processed at a higher rate than your Qualified transactions. This is known as a downgrade. **Your downgrades must not exceed 10% of your overall processing volume.** If they do, you should contact your Processor and ask for assistance. It is the Processor's duty to implement on your behalf the best processing standards required to get the lowest interchange. The problem, however, may have more to do with the way you process your sales orders, than with your Processor. Even then your Processor should be able to help you modify your business practices in a way that will reduce downgrades.

c. **Multiple authorizations.** Real-time transaction processing creates the possibility for multiple authorizations, especially if you are using a dial-up connection. If, during transmission, the connection is lost, the data must be retransmitted which can result in a second authorization. Moreover, your customer's credit limit will be reduced with each authorization request. **Your authorization requests should not be more than 110% of your sales** (for 100 sales you should not have more than 110 authorizations).

XI. Processing Fee Summary.

To eliminate hidden fees and optimize your processing costs, we suggest that you:

a. **Have your pricing done using the interchange-plus model.** The earlier example illustrated the difference between the interchange-plus and the tiered models.

b. **Evaluate on a continuous basis the cost-effectiveness of your own business practices** and their effect on your processing fees. You should establish your own benchmarks and adhere to them. Do not hesitate to request your Processor's assistance, they have contracted with you to do just that.

c. **Make sure that you fully understand your pricing structure.** Before you have signed up with your Processor, you should have asked them to fully explain the basis on which you would be charged for your credit and debit card processing. If you have not done it, contact your Processor now and request it! A better understanding of your pricing will help you set your benchmarks and reduce downgrades.

d. **Perform an independent audit of your processing fees at least once per year.** An independent audit will best show you exactly what your processing costs are and point to areas where you need to work on.

XII. Address Verification Service.

a. **What is Address Verification Service (AVS)?** Address Verification Service (AVS) is a risk management tool for merchants accepting transactions in which neither the card nor the cardholder are present (e.g., mail, telephone order, internet transactions), or in which the card is present but its magnetic stripe cannot be read by a terminal at the point of sale. AVS helps reduce the risk of accepting fraudulent transactions by facilitating the verification of the cardholder's billing address with the card issuer. This address information helps you determine whether to accept a particular transaction or to take further follow-up action.

b. **How does AVS work?** You include the street address and ZIP code of the cardholder's billing address in your authorization request. The Processor compares this information with the respective data at the cardholder's issuing bank, along with other factors (card number, expiration date, etc.) and if approved, issues an AVS code. This additional address information will help you make a better informed decision about whether or not to complete a particular transaction.

c. **How to use AVS?** To request address verification in a card-not-present situation, follow these steps:

i. Enter the billing address as it appears on the monthly statement.

ii. Follow your terminal or computer instructions to enter and send this information.

iii. Research the returned AVS result codes.

d. **AVS Result codes.** One of the following AVS result codes will be returned to you, indicating the response to your address verification request:

Code	Definition	Explanation	Suggested Action
Y	Exact Match	Street address and 5- or 9-digit ZIP code	Generally speaking, you will want to proceed with transactions for which you have received an authorization approval and an "exact match."
A	Partial Match	Street address matches, ZIP code does not	You may want to follow-up before shipping the merchandise or providing the service. Things to look for in these orders: • Larger than normal orders. • Orders containing several units of the same item. • Orders shipped overnight. • Orders shipped to an address other than the billing address.
Z	Partial Match	ZIP code matches, street address does not	
N	No Match	Street address and ZIP code do not match	Typically a strong indicator of fraud, however the cardholder may have moved recently and not yet notified the issuer or the cardholder may have given you the shipping address instead of the billing address. You should: • Call the customer to verify the phone number, the address and whether the cardholder has recently moved. • Call the issuer to determine whether the name, address and telephone number match the information on file. • Use directory assistance or internet search to contact the individual at the billing address and confirm that he or she initiated the transaction.
U	Unavailable	Address information is unavailable for that account number, or the card issuer does not support AVS	The address information for this account is not available; as a result, address verification cannot be performed. You will also receive this response when an issuer does not support AVS. Since you now have no way to verify the address, you must decide whether to investigate further, proceed, or cancel the transaction. One solution is to fax a credit card slip to the consumers requesting a signature be faxed-back to actually verify the order. This may not be the most cost effective means for all international orders, so an order dollar amount perhaps should be established to determine which orders to perform this on.
G*	Global	Address information not verified for International transaction	
R	Retry	Issuer authorization system is unavailable, retry later	The card issuer's authorization system may be down (not working). Try your AVS request again later.

*U.S. merchants use the "G" result code to identify internationally-issued cards.
Caution: When you receive a "partial match" or "no match" AVS response, you should take appropriate steps to assure yourself that the customer is not acting fraudulently. Simply asking the customer for another card will not reduce your risk if the card is being used fraudulently.

Declines can be handled politely by displaying a message that states "We are unable to process your order at this time, if you wish to continue your purchase, please call 1-800…" At that time the merchant may be able to obtain more information from the customer to verify why the address did not match, such as recently moved. The merchant can also ensure their product is shipped via a delivery service that provides a signed receipt to ensure it was received by the proper person.

e. **Why is using AVS important?** Obtaining a positive AVS response is one key step to remedy many "Unauthorized Use" and "Non-Receipt of Merchandise" chargebacks. Without a positive AVS response (on-line) merchants have no dispute rights. AVS is designed to help merchants protect themselves against fraudulent, lost, or stolen credit cards and chargebacks. Visa transactions utilizing AVS are given a better interchange rate than those that do not. You should always be maintaining a customer database or account history files to track buying patterns and compare. Evaluate individual sales for signs of possible fraud. Keep in mind that none of the above by itself means that fraud is being committed, but you should check everything. AVS is not foolproof, but a tool to aid merchants to identify possible fraud orders. It should be combined with your own internal fraud detection tools and with the Card Verification Codes (see below).

XIII. Card Verification Codes.

a. **What are Card Verification Codes?** All major credit card companies and associations have implemented a three- or four-digit security code that is printed on the front or back of each card. This added security measure enables a retailer to verify that the buyer has the actual card in hand during a card-not-present transaction, thus reducing fraudulent transactions. Please refer to the table below for information on the card security codes for each of the major brand.

Card Brand	Security Code	Description
Visa	CVV2 Card Verification Value 2	Located on the back of all Visa cards, the CVV2 consists of the last three digits printed on the signature panel.
MasterCard	CVC2 Card Verification Code 2	CVC2 is a three-digit code printed on the signature panel of MasterCard cards.
Discover	CID Card Identification Number	CID is a three-digit code printed on the signature panel of Discover cards.
American Express	CID Card Identification Number	CID is a four-digit code printed above the card number on the front of American Express cards.

b. **How do Card Verification Codes work?**

   i. **The merchant asks the customer for the Verification Code** and sends it to the card issuer as part of the authorization request.

   ii. **The card issuer checks the Verification Code** to determine its validity, and then sends a result code back to the merchant along with the authorization decision.

   iii. **The merchant evaluates the result code**, taking into consideration the authorization decision and any other relevant or questionable data.

c. **Card verification result codes and suggested actions.**

Result Code	Explanation	Suggested Action
M - match	The number given by the customer matches the one on file with the issuer.	Complete the transaction (taking into account all other relevant or questionable data).
N - no match	The number given by the customer does not match the one on file with the Issuer.	View the “no-match” as a sign of potential fraud and hold the order for further verification.
P - request not processed	Processor is not available.	Resubmit the authorization request.
S - customer reports that there is no Verification Code on the card	Customer cannot locate the security code or is not in possession of the card.	All valid cards are required to have a security code. Consider following up with your customer to verify that he or she checked the correct card location.
U – card issuer does not support CVC2 or CVV2	Issuer is not certified to use CVC2 or CVV2.	Evaluate all available information and decide whether to proceed with the transaction or investigate further.

d. **What else should you know about Card Verification Codes?**

   i. Not all payment processors support security codes. You must check to see if it is available on their system.

   ii. Uncertified card issuers lose chargeback rights for fraudulent Mail Order / Telephone Order (MO / TO) transactions when the Verification Code is included in the authorization message.

   iii. To protect Verification Codes from being compromised, merchants should never keep or store them once a transaction has been completed. Such action is prohibited and could result in fines.

iv. Card Verification Codes are only printed on the cards, they are not contained in the magnetic strip information and do not appear on sales receipts or statements.

e. **Why should you check the Card Verification Codes?** Merchants who check the Card Verification Codes benefit in a number of ways:

i. **Enhanced fraud protection.** Because merchants operating in a card-not-present environment are at greater risk for stolen account number schemes, you need to be diligent in your fraud control efforts. Implementing card security verification can help a merchant differentiate between good customers and fraudsters. It allows you to make a better informed decision before completing a transaction in a card-not-present environment.

ii. **Reduced chargebacks.** Using Card Verification Codes potentially reduces fraud-related chargeback volume by helping you verify that the customer is in actual possession of the card.

iii. **Improved bottom line.** For merchants operating in a card-not-present environment, fraudulent transactions and fraud-related chargebacks can lead to lost revenue and can also mean extra processing time and costs, which often narrow profit margins. Using the Card Verification Codes complements your other fraud detection tools to provide a greater opportunity to control losses and operating costs.

XIV. Credit Card Authentication.

a. **What is credit card authentication?** Both Visa and MasterCard offer authentication services enabling Issuers to verify a cardholder’s account ownership during an online purchase. With Verified by Visa (VbV) and MasterCard SecureCode, consumers are assured that using a bankcard online is as safe as using it at a local merchant. And merchants are fully protected from Issuer chargebacks on transactions which have been fully authenticated. Since the transaction is authenticated by the issuing bank, the merchant will be paid. Merchants no longer need to bear the risk or the cost of fraud.

b. **How does credit card authentication work?** When a cardholder shops at a participating VbV or SecureCode merchant site, the checkout process remains the same until the “Buy” or similar button is selected to place the order. If the card is registered with a participating card issuer, consumers will be asked for their VbV password or their SecureCode issuer specific access credentials. Through this simple checkout process, the Issuer confirms a consumer’s identity in real time.

c. **What do merchants have to do to participate?** Merchants must deploy a software module (referred to as a merchant plug-in) or develop their own software capabilities to support VbV and SecureCode. This software allows merchants to pass cardholder credentials to the cardholder registration servers, and receive responses. Merchants must capture and send authentication data to their processor. Certified Merchant Plug-In (MPI) software vendors work directly with merchants to implement solution.

d. **Why should you implement credit card authentication?** Implementing credit card authentication improves the security of payment transactions in the electronic commerce environment over open networks. It increases both cardholder and merchant confidence in internet purchases, and reduces disputes and fraudulent activity related to the use of payment cards. Specifically, you will benefit from:

i. **Reduced fraud.** The participating merchant gets explicit evidence of an authorized purchase (authentication data) - all with minimal cost impact and time investment.

ii. **Minimized chargebacks.** Once merchants have deployed SecureCode and Verified by Visa, it's up to the Issuer to authenticate its cardholders for online transactions. The authentication data, together with an authorization approval, gives the merchants a transaction that is guaranteed against the most common types of chargebacks - "cardholder not authorized" and "cardholder not recognized" chargebacks.

iii. **Increased cardholder confidence.** MasterCard research shows 90% of online non-buyers worry that their personal and financial information may fall into the hands of hackers. Seventy-one percent are concerned about credit card fraud. Additionally, more than 70 percent of consumers surveyed by Visa indicated that they would be more likely to make purchases at websites that support Verified by Visa.

iv. **Simple set-up.** No special software or digital wallets are required. To get started, all merchants need to do is contact their Processor to ensure processing support and to update their site to include the plug-in application. The initial and ongoing costs are minimal.

XV. Recurring and Installment Payments.

a. **Definitions and distinction.**

i. **Recurring payments.** With recurring payments, the consumer authorizes a merchant or service provider to bill a specific card on a regular basis (e.g., monthly, quarterly or annually). Payment amounts can be fixed or fluctuate, and a payment agreement can exist indefinitely.

ii. **Installment payments.** Installment payment is a single purchase of goods or services billed to an account in multiple segments, over a period of time agreed between a cardholder and a merchant.

iii. **Distinction between recurring and installment payments.** The distinction between the two transaction types is that, a recurring transaction is a payment for goods or services that are received over time, whereas an installment transaction represents a single purchase, with payments occurring on a schedule agreed by a cardholder and merchant. An example for a recurring payment is a cable TV subscription and for an installment payment – a 3-year car lease.

b. **Recurring and installment payments best practices.** The following best practices will help merchants manage recurring and installment transactions effectively:

i. **Allow customers to choose the billing date.** This will help ensure that the cardholder's funds are available.

ii. **Inform the cardholder of the name that will be listed on their credit card statement.** Utilize soft billing descriptors to ensure that cardholders can easily recognize charges on their statements (see next section).

iii. **On the first billing, ask the cardholder for the billing address** as it appears on their statement and if different, ask for the complete "ship to" name and address.

iv. **Provide a clear statement of the cancellation policy** on the cardholder's agreement or on your website. This will help minimize chargebacks.

v. **Provide the cardholder with clear information concerning the billing arrangements** and all charges related to the delivery of goods and services. If billing information is provided online, send a pre-authorization reminder 14 days prior to the processing date.

vi. **For internet transactions, require the cardholder to click on an "Accept" button on the disclosure statement** to confirm they have read your terms and conditions.

vii. **On the first transaction, utilize AVS and Card Verification Codes.**

viii. **Ensure that billing is discontinued immediately upon the cardholder fulfilling the cancellation terms.** Provide the cardholder with cancellation confirmation including when the last billing will occur if it has not occurred already, or if a credit is due, when it will be processed. This will help minimize chargebacks.

ix. **Process credits promptly.**

x. **Ensure that the cardholder is notified when goods or services cannot be delivered or provided on the agreed-upon date.** This will help minimize chargebacks.

xi. **Provide the cardholder with a toll-free phone number for customer service** inquiries and cancellation requests.

xii. **Ensure that an authorization request is approved for all payments** before submitting them for clearing.

c. **Merchant pre-billing notification.** Merchants who provide this type of customer notification prior to submitting an authorization request for a recurring transaction should see fewer disputes when done regularly. Following is a sample of such a notification.

"To: customer name@account.com From: merchant name@account.com
Subject: Recurring transaction notification Date: 28 October 2009 03:15:02 -0500

Dear Customer Name,

This email confirms your authorization* of the transaction
listed below, entered on 10/28/2009 at 3:14:49 AM
has been processed and will be debited from your account.

Transaction Origination Date: 10/28/2009
Name on Account: Cardholder Name
Amount: $14.95
Description: Approved recurring charges on 2009-09-28

*You have authorized Merchant Name Services, Inc and your financial institution to initiate the transaction detailed below. You have acknowledged that the origination of debit or credit transactions to your account must comply with the provisions of local laws. This authorization is to remain in full force and effect until Merchant Name Services, Inc has received written notification from you of its termination in such time and manner as to afford Merchant Name Services, Inc and your financial institution a reasonable opportunity to act on it.

Processed for: Merchant Name Services, Inc
Phone #: 800-111-1111
Email: merchant name@isp.com"

XVI. Billing Descriptors.

a. Types and definitions.

i. **Default billing descriptor.** Default billing descriptor is the description of your company that appears on the cardholder's credit card statement. In order to qualify for the lower interchange rate offered to merchants operating in a card-not-present environment (Visa: CPS; MasterCard: Merit 1), the company name and a customer service number must appear in this field. If your company offers a single product or service this descriptor would be sufficient. For example:

ABC SERVICES 800-111-2345.

ii. **Soft billing descriptor.** The soft billing descriptor allows the description field in the cardholder's statement to be modified to include a more detailed description of the transaction. The merchant's name is usually truncated to three letters plus an asterisk followed by a short description of the service or product being billed. Note that this field is typically limited to 25 characters (excluding the phone number). Be sure to check with your Processor to see if they support this feature and for their format requirements. For example:

ABC* Instant Oil Change 800-111-2345.

iii. **Why should you use billing descriptors?** By utilizing billing descriptors, merchants can make it easier for cardholders to recognize charges on their statements. While it is essential that all merchants make proper use of the description field, this is especially important for merchants who offer more than one product or service. Good billing descriptors:

1. **Reduce customer inquiries.**
2. **Minimize chargebacks.**
3. **Improve your bottom line.**

XVII. Credit Card Processing Resources.

UniBul Merchant Services

www.unibulmerchantservices.com

Our website offers a variety of free card processing manuals, fraud prevention guides, best practices for risk and chargeback management, and much more. Contact us for a free processing analysis and advice for your card acceptance needs.

UniBul Merchant Services Blog

www.blog.unibulmerchantservices.com

Our blog provides articles about credit card processing, industry news, insights, and best practices from merchant services experts.

Merchant Account Services

LinkedIn Group

Our LinkedIn group provides a place for businesses and people interested in using or providing merchant services to share ideas and learn about the industry.

Contact Us

UniBul Merchant Services
p: 617.861.6101
f: 617-684-1709
e: feedback@unibulmerchantservices.com

UniBul Merchant Services on Facebook
UniBul Merchant Services on Twitter

UniBul
MERCHANT SERVICES