

Contents:

Important Contacts (How to Reach Us).....	4
Merchant Point-of-Sale Guidelines.....	5
<i>Fraud prevention for:</i>	
Face-to-Face transactions	
Card-Not-Present transactions	
E-Commerce transactions	
.....	
Navigating Your Statement in One Easy Guide.....	10
Avoiding Supply Scams.....	12
Glossary of Terms.....	13

Important Contacts:

Customer Service - during regular hours, please contact your local provider. For after hours and emergency service, please call1-866-435-3636

Supply Orders.....1-866-435-3636

Visa or MasterCard Voice Authorization.....1-800-291-4840

Discover Voice Authorization.....1-800-347-1111

American Express Voice Authorization.....1-800-528-2121

Diners Club Voice Authorization.....1-800-525-9040

Terminal or Other equipment problems.....1-866-435-3636

Chargeback and Ticket Request Questions.....1-866-435-3636

Mailing Address.....Element Payment Services Corporate Offices
9633 S. 48th Street, Suite 100 Phoenix, AZ 85044

Stolen or Recovered Card Reporting.....1-800-291-4840

Terminal Activation.....1-866-435-3636

Additional Products and services.....1-866-435-3636
customerservice@elementps.com

Terms and Conditions (as amended from time to time) at www.elementps.com/TandC

Merchant Point-Of-Sale Guidelines

Face-to-face transactions- check all card security features

Check the card for a hologram-

A hologram is a three-dimensional symbol in either gold or silver foil that is designed to help deter counterfeiting. The image should reflect light and appear to move when you tilt the card. The Visa hologram is a dove. The MasterCard hologram is two interlocking globes.

Check the expiration date-

The card is valid through the last date of the month. Do not accept an expired card.

Check the valid date-

Some cards will have this feature, in which the card is not valid until the date shown. Do not accept an invalid card.

Check the four digits-

For Visa and MasterCard cards, the first four digits of the embossed card number must match the four digits pre-printed above or below that number.

Check the draft for a clear impression, if you are using a manual imprinter-

This will ensure that you have captured the embossed card account number. Complete the draft with the date, description of merchandise/service, sales tax, total dollar amount, authorization number and signature.

Obtain a manual imprint of the customer's card if you are using an electronic printer and the card can not be magnetic-strip read-

This will ensure that you have captured the embossed card number. Use the manual sales draft to complete the transaction.

Obtain the customer's signature-

Match the signature on the draft to the signature on the back of the card.

If the customer's card is unsigned, request another form of identification with a photo and signature. Request that the customer sign his or her card and then compare the signatures. If the customer refuses to sign, inform him that you are unable to accept an unsigned card for payment and request another form of payment.

Remember... hold the card until the transaction is completed! Retaining the card throughout the transaction enables you to complete all of the security checks without having to ask the customer to re-present his or her card for a signature comparison or possible "call center" procedure. You will avoid check-out delays and ensure a smooth transaction.

What to Look For- Face-to-Face Transactions

Look for physical evidence:

- The hologram is missing or of poor quality.
- The customer's signature does not match the one on the card.
- A MasterCard signature panel does not contain the MasterCard wordmark.
- A Visa card signature panel does not contain the titled Visa pattern.
- The card is warped or has a dull finish.
- The account number and cardholder name are ironed out and the card is embossed with a different number. Evidence of this alteration is noticeable on the back of the card.
- The account number is titled or slanted, or the embossed data spacing is off.
- The printed information is on top of the laminated surface of the card.
- The printing on the back of the card is blurry or distorted.
- Information displayed on the terminal or electronic printer receipt does not match the account number embossed on the front of the card.

Be alert for suspicious behavior:

- The customer appears nervous or overly talkative.
- The customer buys clothing without trying it on for size.
- The customer questions the sales clerk about the floor limit, and then makes several separate purchases that approach but do not exceed the floor limit.
- The customer declines the alterations or delivery although they are included in the price.
- The card is produced from a pocket, not a wallet.
- The customer signs the sales draft in a deliberate or unnatural manner.
- The customer presents only a temporary driver's license without a photo.

Card-Not-Present Transactions – How to Reduce Your Risk of Fraud

In the mail and telephone order business, payment by card is the preferred method – unfortunately it can be a risky one. When neither the card nor the customer is physically present at the point of sale, the merchant experiences the greatest exposure to disputes, chargebacks and fraud.

Guidelines have been developed to help reduce this exposure for mail and telephone order sales.

Remember... For retail or face-to-face sales, the card and the cardholder must be present at the point-of-sale. All sales in which the card is not present either in person, by mail or by telephone order, are taken at your own risk. However, reviewing the following guidelines may help you make more informed decisions on whether to accept such sales at your business.

Authorize every sale on the order date- Authorizations are valid for a specific number of days: Visa – up to 7 days, MasterCard - up to 30 days. Merchandise must be shipped and sales must be deposited within these timeframes, or the authorization will expire. If your shipping date exceeds these timeframes, obtain a new authorization code before shipping the merchandise.

Record the card account number- A Visa card number begins with a 4 and has 13 or 16 digits. A MasterCard card number begins with a 5 and has 16 digits.

Ask for both a billing and shipping address- If the addresses are different, determine whether the difference seems reasonable.

Ask for the customer's phone number – not as a condition for accepting the sale, but as a customer service tool- The phone number enables you to call the customer for various reasons: to inform him or her that merchandise is back ordered, to request another form of payment if the authorization is declined or to verify information if the caller seems unclear about address details.

Ask for the Visa Card Verification Value 2 (CVV2) and MasterCard Card Validation Code 2 (CVC2) number on the back of the card- Turn the card over and read the last three digits, which trail the account number printed in the signature panel (this is the CVV2 or CVC2 code). Note: merchants who request the CVV2 or CVC2 code will receive a match or no match response when entering the transaction into a terminal for processing.

Use the Address Verification Service (AVS)- AVS enables you to compare the billing address provided by the customer with the billing address on file at his card-issuing bank. You receive a verification code indicating a match or partial match. While this is not a guarantee against chargebacks, it allows you to make more informed decisions before shipping. Contact your customer service representative for more information on utilizing AVS.

Do not deposit sales until the ship date- Visa and MasterCard regulations do not permit merchants to receive payment for sales until the goods or services are delivered to the customer. Obtain an authorization on the order date, but do not deposit the sale until the ship date. Visa transactions for custom-ordered merchandise may be deposited on or after the order date, if the merchant has informed the customer that he will be billed prior to shipping.

Maintain a history of fraudulent account numbers or customer names- Store suspect account numbers and customer names in a secure database to cross check when you suspect fraud.

Mail an order confirmation notice to the cardholder prior to shipping- This will not prevent chargebacks, but may reduce the number of inquiries and ticket requests.

Request that your customer service number appear on the customer's credit card statement- Both Visa and MasterCard regulations permit mail and telephone order merchants to place their customer service telephone number where the merchant city would normally appear. This may help the customer recognize the charge when it appears on the statement and reduce the number of ticket requests and disputes. Contact your customer service representative to discuss this option.

Top Ten Warning Signs

of Fraudulent Telephone/Mail Order Transactions:

Hesitant caller- Beware of callers with shaky voices or delayed responses to questions. This may indicate that the caller is not comfortable with the information.

Rush orders- These are a favorite weapon of the “here today/gone tomorrow” schemes.

P.O. boxes and mail receiving services- Most delivery services will not deliver to these addresses. This may indicate lack of permanent address.

Above-average transaction amounts- Merchants often know the amount of an average sale. Be wary of those transactions that greatly exceed the norm.

Purchases that can be easily converted to cash- Examples include electronics, jewelry and leather goods.

Geographic location- The top five states with fraudulent activity are California, Florida, Illinois, New York and Texas.

1-800 return phone numbers- Be suspicious of toll-free telephone numbers when given as the day or evening phone number. Attempt to get a direct line instead.

Multiple orders in a short period of time- Many merchant systems show all orders placed to a certain account or unique customer number. Be especially aware of multiple orders.

Unusual transaction sequences- If the customer typically purchases only accessories and novelty items, but calls in to purchase a new spring wardrobe there may be cause for verification.

Forth quarter- Fraud is always a consideration, but fraudulent activity seems widespread, particularly around the holidays.

Storage of Drafts

Merchants must store all paper copies of sales drafts for 18 months – whether you process manual drafts or electronic receipts. This ensures that you can produce copies of requested drafts and avoid being charged back for non-receipt of requested item. Store your drafts in their original batches, in date order, for easy location. Mail and telephone order merchants may benefit from facsimile drafts, from which we can produce a facsimile of sales receipt for mail and telephone orders using information originally provided in settlement. Contact your customer service representative for more information on this service.

E-Commerce Transactions-

What to be Alert For

When processing electronic commerce transactions, be alert for:


- **A first purchase** which is also typically the sole purchase made, allowing criminals to minimize the possibility of identification associated with re-occurring purchases
- **Larger than normal orders** that maximize purchases on time-limited stolen or bogus payment card accounts
- **Orders consisting of multiples of the same item or big-ticket items** that maximize resale value and profit potential
- **Orders shipped rush or overnight** to deliver fraudulently obtained items as soon as possible for quick resale
- **Orders from Internet addresses using free e-mail services** that do not require a billing relationship or verification that an account was opened by a legitimate cardholder

Develop and maintain customer databases to track buying patterns and identify changes in buying behavior such as:

- **Transactions charged to similar account numbers** as fake account numbers generated by fraud schemes tend to be in sequential order
- **Orders shipped to a single address, but made on multiple cards** to maximize resale value and profit potential
- **Multiple transactions charged to one card over an extremely short period of time** to maximize usage on an account before it is closed
- **Multiple transaction on one card or similar cards with a single billing address**, but multiple shipping address that indicates fraudulent activity by and organized, large scale group
- **Multiple cards used from a single IP (Internet Portal) address** to maximize purchases and profit potential

Navigating Your Statement

in One Easy Guide



ELEMENT PAYMENT SERVICES, INC.
 1-866-435-3636
 9633 S. 48TH STREET SUITE 100
 PHOENIX, AZ 85044
 69000030FB GN 30 0042684 20040731 NNNNYN

ABC MERCHANT
 777 DODGE STREET
 MONTEREY, CA 93940-1426

MERCHANT STATEMENT
 PAGE 1 OF 3
 BILLING STATEMENT FOR
 JULY 31, 2004


CODE:
 PRINCIPAL: 001

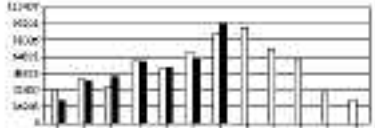
CHAIN: 001
MERCHANT NBR: 1234567
 DBA NAME: ABC MERCHANT

ACTIVITY SUMMARY

TYPE	SALES TOTAL TRANS	CREDIT TRANS	NET AMOUNT
VISA	65,585.52	267	1,595.00
MASTERCARD	31,646.67	132	218.90
CHARGEBACK	0.00	0	97.90

GROSS SALES VOLUME





IMPORTANT ACCOUNT INFORMATION

OUR MISSION: WE WILL SURPASS THE NEEDS OF OUR CUSTOMERS BY PROVIDING PRODUCTS AND SERVICE UNRIVALED IN THE TRANSACTION PROCESSING INDUSTRY. FOR INFORMATION ON OUR PRODUCTS CALL 800-555-1234.

DEPOSIT DETAIL

PROCESS DATE	NBR TRANS AMOUNT	BATCH AMOUNT	3 RD PARTY BATCH AMT	ADJUSTMENT	CHARGEBACK
07/01	13	1,962.40	0.00	0.00	0.00
07/02	13	2,365.00	0.00	0.00	0.00
07/03	7	1,201.20	0.00	0.00	0.00
07/05	20	3,727.90	0.00	0.00	0.00
07/05	14	3,869.80	0.00	0.00	0.00
07/06	19	3,633.00	0.00	0.00	0.00
07/07	9	2,358.40	0.00	0.00	0.00
07/08	7	1,560.90	0.00	0.00	0.00

69000030FB GN 30 0042684 20040731 NNNNYN
 STATEMENT
 MERCHANT NBR:1234567
 OF 3

MERCHANT
 PAGE 2

Statement Explanation

Activity Summary

A summary of each card type processed and paid, switched, or reported. Chargeback volumes are only for card types processed and paid. Graphics are based upon the Sales column.

Deposit Detail

A daily accounting of all batches received and/or processed. The process date is the date we processed the batch. The Net Amount is the amount processed and paid from the batch. Actual payments made may be a combination of multiple Net Amounts.

Third Party Batch Amount Detail

Information on transactions sent to Third Parties for processing and payment.

Adjustment Detail

Batch transactions not processed or paid due to failing transactions edits and any adjustments to payment.

Chargeback Detail

Lists chargeback transactions, including the reason and corresponding documentation case reference number.

Processing Detail

Processing fees listed according to the volume posted to each chargetype. For chargetype definitions, please refer to your Chargetype Guide.

Authorization Detail

Total authorizations processed, including the type of card authorized and method of authorization.

Other Detail

Other services provided and billable items.

Summary

A summary of processing services provided.

Beware of Supply Scams!

Recently, newly signed merchants have been receiving phone calls from businesses representing themselves as the merchant's current credit card processor. The merchants assume that the caller is indeed a representative of their processing bank and consequently do not bother to validate the authenticity of the caller.

The callers state that they are aware that the merchants have new credit card machines and that they need to perform customer upgrades to their machines. In addition, the callers mention that they have printer ribbons or other supplies they can sell to them at a discounted rate. In most instances, the point-of-sale staff assumes the callers are legitimate and agrees to the purchase. The merchants then receive the ribbons and are billed exorbitant prices for basic supplies.

This represents one example of many scams regarding supply companies who are charging exorbitant costs for basic supplies. These supply companies are obtaining merchant information illegally and are taking advantage of current and new merchant customers as well. We have taken precautions to ensure that your business information is not compromised.

Don't be taken advantage of this way and remember to take the following steps to ensure that this does not happen to your business.

- Require all callers to clearly identify themselves.
- Do not give out credit card numbers over the phone.
- Ask if you can phone the caller back if you are suspicious.
- Question suspicious behavior such as nervous and shaky voice patterns.
- Never allow unauthorized personnel to perform service on your point-of-sale terminals.
- Report suspected fraud to a customer service representative only.
- Order supplies from your current bank processor only.

Remember, your point-of-sale staff is your first line of defense against supply scams.

To order your new supplies, contact a customer service representative at 1-866-435-3636.

Glossary of Terms

Automated Clearinghouse (ACH)

One of the group processing institutions that have networked together to exchange (clear and settle) electronic debit transactions.

Address Verification Service (AVS)

A service to help combat fraud in mail order/telephone order transactions by use of cardholder name and address information.

Acquirer

A licensed member of the Visa and MasterCard associations that has an agreement to process the date relating to a transaction from a merchant. The acquirer (your processor) submits data to the associations for settlement.

Affinity Card

Credit cards issued by a bank in conjunction with an organization or collective group; for example, professional, alumni or retired persons' associations.

Assessments

Fees paid by the acquiring member on a quarterly basis to support association advertising and operating activities.

Authorization

A procedure where issuers either approve or decline transaction requests from merchants at the time of sale.

Authorization Terminal

A terminal permitting authorization of a transaction, but not necessarily capturing the transaction data into a payment system, which is also referred to as a P.O.S. terminal.

Card Validation Code 2 (CVC2)

A three-digit value, which appears at the end of the MasterCard card account number printed in the signature panel, that provides a cryptographic check of the card's embossed information.

Card Verification Value 2 (CW2)

A three-digit value, which appears at the end of the Visa card Account number printed in the signature panel, that provides a cryptographic check of the card's embossed information.

Chargeback

A dispute procedure initiated by the card issuer or cardholder after receipt of the initial presentment from the acquirer. The issuer may determine that for a given reason, the transaction was presented in violation of the Rules or Procedures and is therefore eligible to be returned to the acquirer for possible remedy.

Clearing and Settlement

The process of exchanging financial transaction details between an acquirer and an issuer to facilitate posting of a cardholder's account and reconciliation of a customer's settlement position.

Co-branded Card

A customized card product for a specific retail or service merchant that wishes to solicit its customers. These cards contain a Visa or MasterCard logo in addition to merchant logo.

Counterfeit Card

A fabricated card that has been printed, embossed and/or encoded to appear genuine, or a stolen card that has been altered.

Debit Card

A plastic card used to initiate a debit transaction. In general, these transactions are used primarily to purchase goods and services and obtain cash, for which the cardholder's checking account is debited by the card-issuing institution.

Deposit Account

A deposit relationship between a customer and a financial institution. This includes, but is not limited to, demand deposit (checking), savings, share draft and NOW accounts maintained at the institution.

Discount Rate

The fee an acquirer charges its merchants for the processing services that enable the merchants to accept bankcards as a form of payment.

Draft Capture

The process where merchants store and deposit their transactions with their acquiring bank.

E-Commerce

The use of the Internet for business-to-business and business-to-consumer transactions. E-commerce is made possible by encryption technologies such as Secure Socket Layer (SSL).

Electronic Draft Capture (EDC)

A system in which transaction information is electronically stored and submitted to the acquirer for settlement.

Electronic Benefits Transfer (EBT)

The distribution of all government agency benefits electronically via a plastic Electronic Benefits Transfer (EBT) Card.

EDC Terminal

A credit card processing terminal which supports Electronic Draft Capture.

Exception Processing

Any special requirements a merchant has in terms of reporting, accounting, programming or other areas, which necessitate additional work by the processor or acquiring bank.

Expiration Date

The date embossed on the card beyond which the card must not be honored.

Interchange

The exchange of transaction data between acquiring and issuing institutions.

Interchange Fee

The amount paid by the acquirer to the issuer on each sales transaction. MasterCard International and Visa U.S.A. independently establish interchange fees for their networks.

Internet

An enormous system of linked computer networks, worldwide in scope, that facilitates data communication services such as remote login, file transfer, electronic mail, the World Wide Web and newsgroups.

Internet Address

The unique, 32-bit address assigned to a computer that is connected to the Internet, represented in dotted decimal notation.

Issuer

The institution (or its agent) which issues the card to the cardholder.

Merchant

A government agency, retailer or any other person, firm, or corporation that, pursuant to a merchant agreement, agrees to accept credit and/or debit cards when properly presented.

Merchant Agreement

A written contract between a merchant and a bank containing their respective rights, duties and warranties, with respect to acceptance of the bankcard and matters related to the bankcard activity.

Non Face-to-Face Transaction

Any transaction wherein the card is not presented; for example, a mail/telephone order.

Payment Gateway

A means by which users of one computer service or network can access certain kinds of information on a different service or network.

Point-of-Sale (POS) Terminal

A device placed at the point-of-sale, connected to a system via telecommunication lines, designed to authorize, record and/or forward sales transactions by electronic means.

Off-line Debit

A debit card transaction performed with a Visa Check Card or MasterCard MasterMoney Card where the purchase is debited from the cardholder's checking account after clearing and settlement. The card does not have to be present for off-line debit transactions.

On-line Debit

A debit card transaction performed with an ATM card and personal identification number (PIN) in a card-present environment. These transactions are authorized and posted to the cardholder's checking account simultaneously.

Reference Number

The number assigned to each monetary transaction in a cardholder billing system. Each reference number is printed on the monthly statement to aid in the retrieval of the document, should the cardholder question it.

Retrieval Request

The request for either an original sales slip or legible reproduction of a sales slip as identified in the electronic record.

Secure Socket Layer (SSL) Encryption

An Internet security standard that is widely supported by leading Web browsers and Web servers.

Truth in Lending Act (TILA)

A law that limits cardholder liability for unauthorized charges to his or her account.

Web Browser

A program that runs on an Internet-connected computer and that provides access to the riches of the World Wide Web (WWW).

Web site

On the Web, a computer system that has a recognized domain name and that runs a Web server for publishing documents on the Web. A Web site generally makes many Web pages available.

Zero Floor Limit

A floor limit that requires all cardholder transactions to be sent to the issuer for authorization.