

**UMS Banking** <sup>SM</sup>  
Payment Processing Services

750 Fairmont Avenue, 2nd Floor  
Glendale, CA 91203

PRSRT STD  
U.S. POSTAGE  
**PAID**  
LOS ANGELES, CA  
PERMIT NO. 3344

Phone: 1-800-324-8323  
Fax: 1-818-246-0902  
Email: info@umsbanking.com

Visit our Website:  
[www.umsbanking.com](http://www.umsbanking.com)

**Referral Program LAUNCHED!**  
Bring us a friend...  
We'll give you \$25.00



Volume 2, Issue 1  
First Quarter 2006

**Vital Industry Tips...**

**1. For Internet or Mail Order/Telephone Order (MOTO) Merchants...** credit card acceptance is paramount to your business. But success means dramatically reducing your exposure to fraudulent cardholder activity. How can you protect yourself from cardholders whose intent it is to defraud you? The following are some suggestions. Although there's no guarantee that elimination of all cardholder fraud is possible, close attention to these guidelines is a most effective way of significantly reducing the likelihood that your business will be exposed.

**2. Obtain a Signature!** A chief reason that chargeback ratios are high for Internet and MOTO merchants is the inability to obtain a signature at the time of the transaction. Finding a means of obtaining the cardholder's signature is an excellent way to link the sale to the cardholder and help to mitigate a dispute that may otherwise lead to chargeback. For example, if your business is shipping hard goods, request a signature at the time of delivery or include with the shipment a return-postage-paid acknowledgement of receipt-of-merchandise, to be signed and returned.

**3. Use AVS & Caller ID!** These services allow MOTO merchants to identify possible questionable activity. If AVS does not match the street address and the zip code, then you should not process the transaction until you have done additional research. Caller ID may help you to identify fraudulent cardholders in a similar manner.

**4. Use Internal Edits!** Customers using fictitious account numbers will input one number after another until they receive an authorization. Have internal edits check for multiple transactions attempted in which the last 3 or 4 digits are different for each transmission. Such a system may also be programmed to flag card numbers for which a chargeback has been previously associated.

**5. Flag Recurring Transactions!** If you charge your customers on a recurring basis, make sure that you identify each transaction as a recurring transaction. Check with your vendor or software company to find out if your software system will allow this. By flagging transactions as recurring, you help protect from chargebacks for "duplicate processing." Providing cardholders with a clearly marked and easy-to-use cancellation form helps them to notify you if they decide to cancel services.



**UMS Banking** <sup>SM</sup>  
Payment Processing Services

...your path to superior service & technology

## MERCHANT'S NEWS QUARTERLY

### Contacts:

**1 (800)324-8323**

#### New Account Referral:

Breeann Kersey  
- Leads Manager

#### Sales Questions:

Todd Robinson  
- Sales Manager  
Akisha Serrano  
- VP Sales

#### Operations Issues:

Frank Lopez  
- VP Operations

### Help Desk:

#### Customer Care Center:

**1(800) 866-1881**

Terminal Assistance  
Statement Questions  
Install & Training  
Account Changes

**OUR TECHNICAL  
STAFF IS  
READY TO  
SERVICE  
YOU!**

Ask your Sales Representative  
about:

Visa® Gift2Go<sup>SM</sup>  
Reloadable MasterCard®  
Cell phone, Ringtone and  
Prepaid Telephone Cards!

### President's Message



David Jensen, President

#### TO OUR VALUED CUSTOMERS:

A new year is beginning with a renewed dedication to our reputation of personal customer service for all of our merchants. I personally sent out a letter and a survey to see how we were doing recently. I was pleased to see that we are keeping most everyone happy with fast, hassle-free service.

Internally, we've upgraded our speed of service by adding more personnel and quicker computer systems for reporting. We have new products to maintain compliance with industry security advances and ever-changing consumer demands, including gift cards, check readers, etc.

I wish you all the best for a prosperous 2006!

### VERIFONE'S "PORTABLE POWERHOUSE" THE VX610

#### Why Would a Retail Merchant Go Wireless?

- Eliminates messy wiring at Point-of-Sale.
- "Always On" connectivity gives you 2 second response time.
- Saves counter space.
- Long life battery makes all-day use possible.
- Accepts Debit and Credit in a wireless mode.

#### Wireless You Can Count On!

- Integrated dial-up modem can keep you connected when there isn't a wireless signal.
- Top performance antenna provides connectivity in many hard to reach places.

#### Features that Complete the Package

- Modular design allows you to take advantage of the latest technologies and upgrade when new ones become available.
- Integrated PINPad allows clerks to easily hand over the device to customers for PIN entry, or you can purchase a swivel base.

**WIRELESS  
That WORKS!**



- Convenient applications available such as "Time and Attendance" employee software, or "Age Verification" software.

#### Add Portability and Flexibility

- Perfect for Home Deliveries, Kiosks, Drive-thru Windows.
- High reliability at Trade Show venues.
- Adds an additional Point-of-Sale lane without the fuss or muss of a phone line or wiring.
- Perfect for those "One-time" events that do not have phone access such as charities.

#### Ease of Use and Familiar Design

- High speed thermal printer with "clam shell" design and drop-in paper loading eliminates jams.
- Easy prompt window makes training employees simple.

**Call Today!  
1 (800) 324-8323**

## Merchants Are Now Liable For Security Breaches On Cardholder Information

Merchants can be held financially responsible for a fraudulent transaction even if it has been approved by the card issuer! The Payment Card Industry (PCI) Data Security Standard lists 13 requirements that must be adhered to:

#### Build and maintain a secure network:

1. Install and maintain a firewall.
2. Don't use vendor-supplied defaults or system passwords.

#### Protect Cardholder Data:

3. Protect stored data.
4. Encrypt transmission of data across public networks.

#### Maintain a Vulnerability Management Program:

5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

#### Implement Strong Access Control Measures:

7. Restrict data access by need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

#### Regularly Monitor and Test Networks:

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

#### Maintain an Information Security Policy:

12. Maintain a policy that addresses information security, including the safe guarding of credit card slips.
13. In addition, retailers in California must adhere to card number truncation on slips.

## MERCHANT'S NEWS QUARTERLY

### Contacts:

**1 (800) 324-8323**

#### New Account Referral:

Breeann Kersey  
- Leads Manager

#### Sales Questions:

Todd Robinson  
- Sales Manager  
Akisha Serrano  
- VP Sales

#### Operations Issues:

Frank Lopez  
- VP Operations

### Help Desk:

#### Customer Care Center:

**1(800) 866-1881**

Terminal Assistance  
Statement Questions  
Install & Training  
Account Changes

**OUR TECHNICAL  
STAFF IS  
READY TO  
SERVICE  
YOU!**

Ask your Sales Representative  
about:

Visa® Gift2Go<sup>SM</sup>  
Reloadable MasterCard®  
Cell phone, Ringtone and  
Prepaid Telephone Cards!

### President's Message



David Jensen, President

#### TO OUR VALUED CUSTOMERS:

A new year is beginning with a renewed dedication to our reputation of personal customer service for all of our merchants. I personally sent out a letter and a survey to see how we were doing recently. I was pleased to see that we are keeping most everyone happy with fast, hassle-free service.

Internally, we've upgraded our speed of service by adding more personnel and quicker computer systems for reporting. We have new products to maintain compliance with industry security advances and ever-changing consumer demands, including gift cards, check readers, etc.

I wish you all the best for a prosperous 2006!

**VERIFONE'S**  
"PORTABLE POWERHOUSE"  
THE Vx610

### Why Would a Retail Merchant Go Wireless?

- Eliminates messy wiring at Point-of-Sale.
- "Always On" connectivity gives you 2 second response time.
- Saves counter space.
- Long life battery makes all-day use possible.
- Accepts Debit and Credit in a wireless mode.

#### Features that Complete the Package

- Modular design allows you to take advantage of the latest technologies and upgrade when new ones become available.
- Integrated PINPad allows clerks to easily hand over the device to customers for PIN entry, or you can purchase a swivel base.
- Convenient applications available such as "Time and Attendance" employee software, or "Age Verification" software.
- High speed thermal printer with drop-in paper loading eliminates jams.
- Easy prompt window makes training employees simple.

**WIRELESS**  
*That WORKS!*



#### Wireless You Can Count On!

- Integrated dial-up modem can keep you connected when there isn't a wireless signal.
- Top performance antenna provides connectivity in many hard to reach places.

#### Add Portability and Flexibility

- Perfect for Home Deliveries, Kiosks and Drive-thru Windows.
- High reliability at Trade Show venues.
- Adds an additional Point-of-Sale lane without the fuss or muss of a phone line or wiring.
- Perfect for those "One-time" events that do not have phone access such as charities.

**Call Today!**  
**1 (800) 324-8323**

## Merchants Are Now Liable For Security Breaches On Cardholder Information

Merchants can be held financially responsible for a fraudulent transaction even if it has been approved by the card issuer! The Payment Card Industry (PCI) Data Security Standard lists 13 requirements that must be adhered to:

#### Build and maintain a secure network:

1. Install and maintain a firewall.
2. Don't use vendor-supplied defaults or system passwords.

#### Protect Cardholder Data:

3. Protect stored data.
4. Encrypt transmission of data across public networks.

#### Maintain a Vulnerability Management Program:

5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.

#### Implement Strong Access Control Measures:

7. Restrict data access by need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

#### Regularly Monitor and Test Networks:

10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

#### Maintain an Information Security Policy:

12. Maintain a policy that addresses information security.
13. In addition, retailers in California must adhere to card number truncation on slips.