PULSATIONS

pulse®
Bringing Value to Electronic Payments℠

PULSE Conducts Participant Survey

Fraud Protection and Debit Usage Attract Attention

In late 2006, PULSE commissioned Analytica, Inc. to conduct a survey of PULSE financial institution participants. The goal of the study was to learn more about the challenges participants are facing in the payments area, the benefits they are receiving from electronic payments and the level of service PULSE is providing.

Not surprisingly, concern about debit card fraud and the effect it is having on issuers' bottom lines was the predominant theme in the survey results. This theme was woven throughout participants' responses to a wide variety of questions. Another area of issuer focus is new payment technologies and the opportunities they present.

"PULSE periodically conducts participant surveys in order to better understand the challenges and opportunities that financial institutions face, as well as how PULSE can better help them cope with changes occurring in the industry," said Cindy Ballard, PULSE executive vice president. "These surveys also provide valuable insights into how we are performing as a service provider and where we can focus our attention to deliver greater value going forward."

Payment Trends

Analytica conducted telephone surveys of a representative sample of 210 participants with a wide variety of types and asset sizes. Respondents included financial institutions that are new to the network, as well as those that have been participants over the medium and long terms.

Among the changes that have occurred in the payments industry in the last few years, increased fraud was seen by survey participants as the most significant trend, with 69 percent of respondents citing it as having the biggest impact on their institutions. Eighty-three percent of credit unions surveyed cited fraud as having the greatest impact on their business, while 65 percent of banks and 50 percent of savings institutions ranked fraud as the most significant concern.

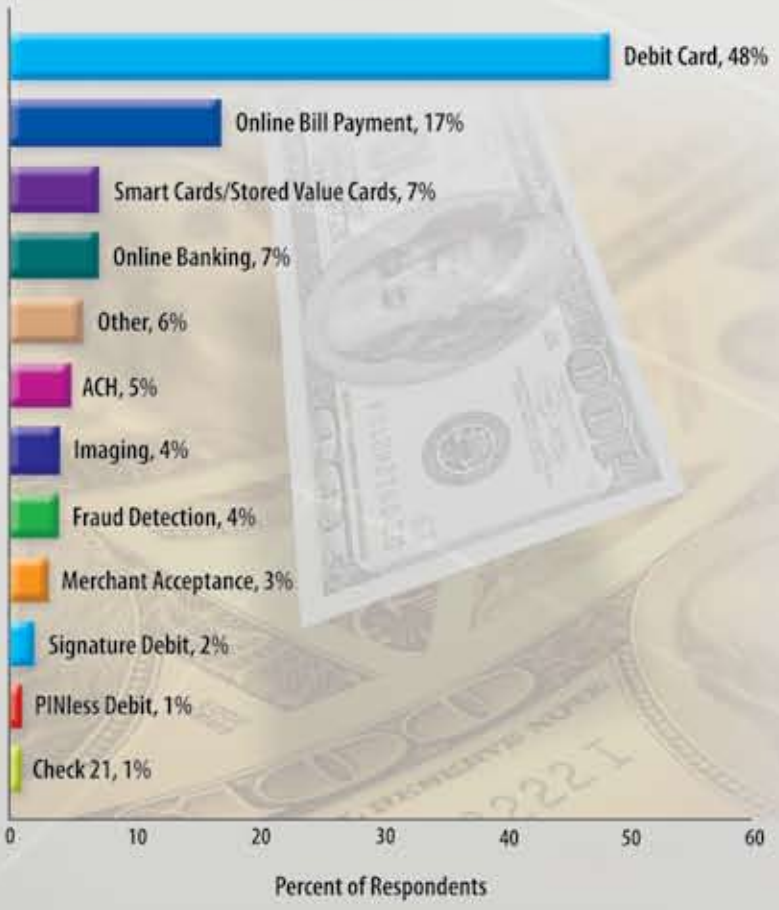
The second most influential trend noted by participants is the growth in debit card usage. One respondent said they had seen "much broader acceptance of that access vehicle in the consumer market."

When asked which payment product innovations have had the greatest positive impact on their organizations, a total of 50 percent of study participants cited debit cards or signature debit, and 24 percent mentioned online bill payment and online banking.

PULSE also asked participants to rate, on a scale of 1 to 10, the importance of several services the network provides, as well as PULSE's effectiveness at providing those services. Respondents see protection from fraud and risk as the most important service, giving it an average rating of 9.5 on a 1-to-10 scale. This was followed closely by providing cardholder access to ATMs and PIN debit terminals and effectiveness at switching and settling transactions.

(continued on page 6)

Payment Innovations with Greatest Impact on Financial Institutions



Source: *2007 PULSE Participant Study*, Analytica, Inc.

June is PULSE ATM & Debit Card Safety Month – Volume is Up and Risk is, Too

Debit card transactions, at both the ATM and point of sale (POS), are becoming a preferred payment method for consumers, due to ease of use and growing acceptance.

However, this convenience can also pose risks in the form of personal safety, theft and fraud. PULSE established June as **ATM & Debit Card Safety Awareness Month** seven years ago to highlight safety for debit card users. Today, 72 percent of all accounts have debit cards, according to the PULSE *2007 Debit Issuer Study*, and PULSE wants to re-emphasize safety awareness to financial institution participants.

Financial institutions realize that debit cards can help maintain and grow account holder relationships. There are many steps the financial services industry can take to reduce the safety risks for their debit card users, one of which is to educate consumers so they can better protect themselves.

(continued on page 5)

Dave Schneider

"PULSE is committed to maximizing value and service for all network participants. This commitment drives us not only to learn more about the needs and wants of financial institutions, but to continually seek ways to better serve those needs."

Dear PULSE Participant,

Access to leading industry and consumer research is one of the key value-added benefits of PULSE participation. In the last issue of *PULSATIONS,* we summarized the results of the *2007 Debit Issuer Study.* This comprehensive study of the U.S. debit card industry provides valuable information relative to debit program performance, interchange rates, fraud and more. If you have not downloaded your executive summary of this extensive study from the PULSE Web site, I urge you to do so.

The current issue of *PULSATIONS* includes detailed results from the *2007 PULSE Participant Study* (see story beginning on page 1). Conducted by Analytica, Inc. on behalf of PULSE, this extensive survey provides answers to a wide range of debit-centric questions from a representative sample of PULSE participants.

When asked which innovations in electronic payments have had the biggest positive impact on their institutions, 48 percent of survey respondents cited debit cards. Debit represents a substantial revenue source for financial institutions.

Not surprisingly, increased fraud was identified by 68 percent of PULSE participants surveyed as the industry trend that has had the most significant impact on their institutions over the past few years. In the past year, PULSE has introduced new products aimed at helping our network participants combat debit fraud at all levels, and is launching other projects in this area that you will be hearing more about in the coming weeks and months.

PULSE is committed to maximizing value and service for all network participants. This commitment drives us not only to learn more about the needs and wants of financial institutions, but to continually seek ways to better serve those needs. For example, our experienced and knowledgeable personal relationship managers can assist you in examining the profitability of your payments portfolio and determining the best product mix for your institution.

We work hard to deliver best-in-class service to all of our financial institution participants. If you have suggestions about how PULSE can enhance any aspect of our service, please let me know personally.

As always, thanks for your continued support of the PULSE network.

Sincerely,

Dave Schneider

Dave Schneider
President

Plan to take advantage of one or more of the many educational opportunities that PULSE is offering in the coming months. For more information on all PULSE educational offerings, please refer to the Financial Institutions section of the PULSE Web site at www.pulse-eft.com.

PULSE Academy℠ Webinars

Redefining the Profitability of Your ATM Portfolio – *2006 ATM Deployer Study*

Thursday, June 7

The latest ATM study, conducted by Dove Consulting and co-sponsored by PULSE, reveals an evolving business model and provides the most comprehensive assessment of the state of the U.S. ATM industry. Led by Judith McGuire, PULSE's vice president of retail services, this session will cover such topics as historical, current and future transaction levels; adoption of and interest in advanced ATM functionality; benefits and challenges of check imaging at the ATM; advanced software and ATM technologies; trends in surcharging and surcharge-free access; and deployer economics.

PULSE New Participant Webinar

Tuesday, May 15

The New Participant Webinar gives financial institutions that are new to PULSE an opportunity to learn more about the benefits, products and services they receive as a participant. This Webinar provides an overview of the PULSE network, including pricing and optional services, educational opportunities and numerous value-added services options. This convenient session is a great way for new financial institutions or staff members new to the industry to find out how to make the most of their ATM/debit programs. The Webinar is available at no cost.

Coming Soon . . .

Debit Card Profitability Series

This new four-part Webinar series will focus on major factors impacting debit card programs and profitability. Participants will receive information on how to stay competitive in this ever-changing marketplace and find key strategies for business success. This series will help participants analyze their current program, learn how to maximize their debit card portfolio, discover how to avoid risks associated with the product and understand costs. Participants will also gain an understanding of debit cardholder demographics, as well as how cardholders respond to various debit card features.

Please contact Melissa Voelkner at 800-282-8963 with questions regarding all seminars and training.

¿Habla Español?

Q&A

Q: Why study financial practices of the Hispanic population?

A: Research reveals that 36 percent of Hispanics polled do not use traditional financial institutions to meet their needs. More than 38 percent of this group believe they simply have no need for such services.

For assistance in reaching the Hispanic market, visit www.pulse-eft.com or call 800-420-2122.

Source: ***The Untapped Market: A Multicultural Study of Consumer Preferences***

New Phishing Scheme Targets Dual Authentication Signup Process

Lisa King, Public Relations Manager, SecureWorks, Inc.

In November 2006, SecureWorks, a leading provider of managed information security services, announced it had disabled several phishing schemes that were using the dual authentication sign-up process to lure banking and credit union customers to bogus phishing Web sites.

These phishers were directing potential victims to sign up for their financial institution's new dual authentication solution – ironically, a solution intended to help protect their online banking activities from fraud. The phishing scam used e-mail to target financial institutions' account holders, asking them to enter their account number and personal identification number (PIN) in order to register for a new dual authentication code and phrase. The e-mail explained that a dual authentication code and phrase were required to conduct online banking, as directed by the Federal Financial Institutions Examination Council (FFIEC).

In October 2005, the FFIEC issued a "guidance" requiring banks and credit unions to strengthen the method by which Internet banking customers verify their identities. The document is designed to help combat risks resulting from phishing, pharming, malware and other increasingly sophisticated compromise techniques.

This guidance, which replaced the FFIEC's *Authentication in an Electronic Banking Environment* issued in 2001, does not endorse any particular type of two-factor authentication. Rather, it addresses the need for risk-based assessment, customer awareness and implementation of appropriate risk mitigation strategies, including security measures to reliably authenticate customers accessing their financial institutions' Internet-based services. The guidance required financial institutions to have stronger authentication in place by December 31, 2006. Now it appears that this very requirement was used in the evolution of sophisticated compromise techniques.

Two-Factor Authentication

Historically, most online banking applications have used single-factor authentication, requiring the user to provide known information such as a password. But more sophisticated authentication techniques involve two or more factors. For example, PIN debit transactions involve two identification factors: the debit card itself (something the user *has*) and the PIN (something the user *knows*). Other types of authentication include something the user *is* (the user's fingerprint or retinal scan, for example) and something the user *does* (such as the user's signature).

Although few financial institutions have begun using true two-factor authentication to verify the identity of online banking customers in response to the FFIEC guidance, many are utilizing additional layers of authentication, such as security questions that are chosen in advance by the account holder. It is this latter type that the phishing scheme attempted to mimic, and thus convince account holders to reveal highly sensitive information.

Dual Authentication Scam

This scam was extremely clever, using the FFIEC's dual authentication guidance – which was developed to protect online banking from fraud – to try to scam potential victims. The perpetrators of the attack used a combination of phishing and hacking in their attempt to commit fraud.

SecureWorks discovered that the phishers hacked vulnerable computers and used them as platforms to host the bogus phishing sites. The compromised host servers were located in Europe and the Far East, and were being used as fallback host servers. This meant that, when one phishing site was taken down, a duplicate phishing site was activated. SecureWorks efforts also revealed that the phishers were using the compromised servers to host scams against several different financial institutions, not just one.

As a result of SecureWorks' relationship with the United States Computer Emergency Readiness Team (US-CERT), as well as several foreign CERT teams and incident response teams within some of the world's largest Internet service providers, SecureWorks was able to get the compromised servers in Europe and the Far East taken down.

Protecting Your Institution

Unfortunately, as consumers become more educated, phishing schemes also become more innovative. Financial institutions of all sizes need to be constantly on the lookout for such scams. If they don't have the resources in-house to deal with them, they need to have an experienced IT security provider that can quickly and effectively terminate the scam.

SecureWorks recommends that companies take the following steps to protect themselves against phishing:

1. Shield your employees and mail servers against phishing attacks by "dropping" (deleting) e-mails sent from non-existent addresses and filtering e-mails based on phishing-related content.
2. Send e-mails using the same "From" domain as your Web site (for example, customerservice@secureworks.com), and monitor bounces from that address sent back to your mail server. A sudden increase in bounce-backs will serve as an alert that phishers may be "spoofing" your e-mail address (forgery of an e-mail header so that the message appears to have originated from someone other than the actual source).
3. Use transaction-based, rather than session-based, authentication. Financial institutions may want to employ a combination of the two types, using session-based authentication to allow browsing of statements and balances but requiring transaction-based authentication to initiate payments or transfers.
4. Disable mail relay on e-mail servers to prevent the propagation of fraudulent e-mails.
5. Educate your account holders about phishing, and urge them never to access your Web site from a link provided in an e-mail, but to do so only by typing in the actual Web address.

SecureWorks is a provider of managed security services, serving more financial institutions than any other security vendor. For more information on this and other topics related to information security, visit www.secureworks.com.

Discover® Debit Business Card Focuses on Small Business Support Agreement

"Small businesses are widely considered one of the most promising markets in the electronic payments industry today . . ."

Issuance of business debit cards represents a significant untapped opportunity for many financial institutions. The Discover Debit Business Card offers a variety of special features that can help debit card issuers penetrate this rapidly growing market.

Discover Debit business and consumer card offerings give cardholders added security and convenience features such as:

- Acceptance at more than 4 million merchant and cash access locations throughout North America;
- Three ways to get cash – cash disbursements, ATMs and Discover Network's unique Cash Over Program;
- Access to an identity theft specialist 24/7, plus an identity theft recovery kit and up to $2,500 in financial relief (subject to a $250 deductible)*;
- Travel assurance services, including a lost key/luggage service and an emergency cash/airline ticket service;
- A lowest purchase price guarantee that reimburses cardholders for the price difference if they find an identical item at a lower price within 60 days of making the purchase; and
- A card and document registration service that notifies all of the cardholder's payment card issuers within 24 hours and automates re-issuance of replacement cards.

In addition to these features, Discover Debit offers business cardholders access to professional consulting services, as well as business advisory services in the form of a Small Business Guide. The professional consulting services, accessible online or by phone at no charge, include:

- **Human Resources Consultant** – offers professional guidance through virtually every facet of HR, including recruitment, performance, regulatory compliance, change management and COBRA and FMLA administration; and,
- **Attorney on Call** – enables business owners to query licensed attorneys on a wide range of topics such as contracts, immigration, employment laws and employee benefits.

"Small businesses are widely considered one of the most promising markets in the electronic payments industry today, and the Discover Debit Business Card's unique features are designed to appeal specifically to that market," said Jeff Brandt, vice president, Discover Debit Products and Management. "By differentiating the cardholder features, PULSE and Discover Network aim to help financial institutions in their efforts to attract new business debit cardholders."

Small Business Guide

The Discover Debit Small Business Guide is a detailed and extensive online resource for small business owners that may not have access to such information through traditional channels. The guide provides a wealth of information and tools to help business owners in every stage of a company's life cycle, from planning and start-up to financing, marketing, staffing and even closing a business. Other topics include winning government contracts, managing employees, controlling taxes, managing business finances and protecting assets.

The Discover Debit Small Business Guide also includes forms, templates and other ready-to-use tools to help business owners get the job done faster and easier, including:

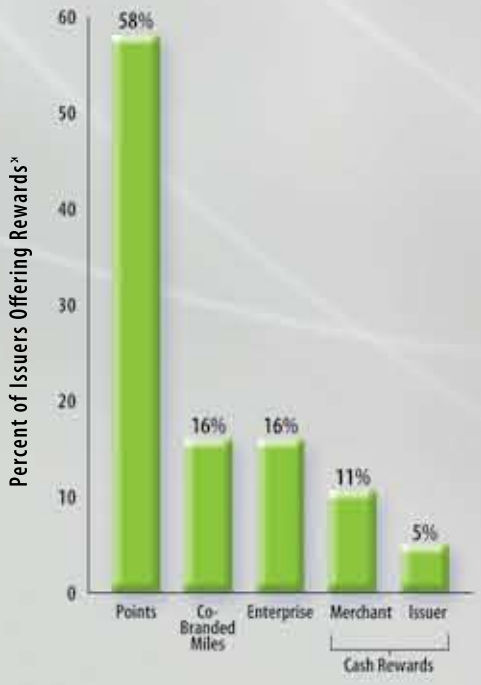
- **Model business documents** – Customizes sample letters, contracts, forms and policies;
- **Financial spreadsheet templates** – Tools to help manage business finances, from balancing the check book to creating financial statements;
- **Checklists** – Information business owners need to help them perform important tasks such as determining whether a business qualifies for a home office tax write-off or conducting an employee termination interview; and
- **Official Government Forms** – A selection of the forms and publications commonly used by small business owners when filing taxes or contracting with the federal government.

For information, visit the Discover Debit Business Resource Center at http://debit.discovernetwork.com/public/cardholders/businesses.html.

*Not available to NY residents.

Debit Rewards Take Center Stage

Types of Rewards Programs Offered



*Percentages do not total to 100 percent because some issuers offer more than one type of program.

Source: *PULSE 2007 Debit Issuer Study*

Offering debit rewards is among issuers' top priorities and is viewed by many as a competitive necessity. This finding was revealed in PULSE's *2007 Debit Issuer Study*. Results were released in February.

The study found that debit rewards program options are increasing, and that debit card issuers are implementing a variety of program types with varying accrual rates and redemption values. Program types include those that award points, airline miles and cash, as well as an emerging program type that rewards an account holder's overall relationship with an institution.

Of the 37 percent of study respondents who offer debit rewards, 63 percent offer rewards only for signature debit. However, issuers also are increasingly offering incentives for PIN transactions.

The PULSE study revealed that debit rewards are having a positive impact on financial institutions' bottom lines, although there remains significant upside potential in terms of enrollment, usage and profitability. Enrollment in opt-in programs is relatively low, with study participants reporting penetration rates of 3 to 15 percent. But study participants with established programs report notable increases in transaction activity and retention. The average lift in transaction activity for traditional points programs was reported to be approximately 25 percent.

"Our card activation rate is 70 percent higher, transaction activity is double and our ratio of signature to PIN transactions is higher," said one large bank of its co-branded miles program.

"Ninety percent of cards enrolled are active, and those cardholders are making 50 percent more signature debit purchases per month. Turnover is less than 7 percent," said another financial institution, also referring to a miles-based program.

Addressing its cash rewards program, a third large bank that participated in the PULSE study said it had seen 29 percent growth in average transaction size and a 15 percent decrease in closed accounts.

Most issuer cash rewards programs and enterprise rewards programs are too new to evaluate their impact on customer relationships.

For more information on PULSE's *2007 Debit Issuer Study*, please visit www.pulse-eft.com.

June is PULSE ATM & Debit Card Safety Month – Volume is Up and Risk is, Too (continued from page 1)

Cardholders should think about fraud prevention when they use their debit cards and treat them with the same care they would cash. For example:

- **Guard your PIN number –** Don't let strangers in line behind you see your PIN, and don't give it to friends or family members, even "just once." Debit card fraud is often a result of someone the card owner knows using the card, so take care to prevent it from happening to you. Never let a store clerk enter your PIN for you on a transaction. Always ask for the receipt for a PIN or signature debit transaction.
- **Beware of unsolicited e-mails –** E-mail is a common channel for fraud. If anyone asks for your PIN over the telephone, online or through e-mail, don't provide it. No financial institution or legitimate merchant will ask for your PIN, so assume any request for it is an attempt at fraud.
- **Guard yourself while at an ATM –** Take a look around. Be sure no one is nearby when you drive up in your car, or that no one is standing near you if you walk up. If it is dark or you are alone in the area, take special care to check around you, including behind walls, trees or bushes. If you feel afraid, don't take a chance – cancel your transaction and get away. If you are walking, don't linger, but do not leave the ATM until you put your cash away. If someone follows you, either on foot or in a vehicle, go to a crowded, well-lit area immediately and call the police.
- **If it doesn't feel right, it probably isn't –** Look for possible fraudulent devices attached to an ATM. If the ATM itself looks altered or has something that appears to be attached to it, or if your card doesn't slide easily into the slot, don't use it.
- **Guard against online fraud –** Look for secure transaction symbols when shopping online to ensure that your personal and account information are protected. Such symbols include a gold padlock icon in the lower right-hand area of the screen and a Web address that begins with "https" rather than "http." Never provide your PIN for an online transaction, and always log off from any site after you make your purchase. If you can't log off, shut down. Do not reply to unsolicited e-mail or pop-up messages.
- **Keep track of your debit card information –** Be sure you keep your account number and the phone number of your financial institution in a safe place so you can call immediately if your card is lost or stolen. Never write your PIN on your card, and don't use an easy-to-guess PIN such as your street address or your birth date. Don't leave mail in your mailbox or throw away bank statements without shredding them. Keep your receipts, and frequently check your account online or by phone so you can spot fraudulent transactions. Notify your financial institution right away if you see anything suspicious.

ATM owners also can help:

- **Ensure that your ATMs are maintained frequently –** Regular maintenance checks will help prevent anyone from tampering with or attaching anything onto an ATM for the purpose of obtaining secure information from cardholders.
- **Clean up the location –** Be sure your ATMs are placed in well-lit, clean, open environments, without dark corners or bushes nearby that could be hiding places for crooks.
- **Educate your cardholders –** Regularly provide information about ATM and debit card safety to your cardholders. You may also want to consider posting a general warning about phishing in a prominent place on your Web site.

To assist financial institutions in promoting ATM and debit card safety to cardholders, PULSE offers ATM and debit card safety materials, including statement inserts, card protector sleeves and Web brochures. See the PULSE Bulletin on page 6 for details and ordering instructions.

PULSE BULLETIN

As part of our ongoing ATM & Debit Card Safety Awareness Campaign, PULSE offers a variety of materials that financial institutions can order and distribute to cardholders. The materials listed below are available for order on the PULSE Web site. Simply visit www.pulse-eft.com and click Communication Materials under the ATM/Debit Safety tab.

ATM & Debit Card Safety Statement Inserts

These inserts offer important tips on ATM and debit card safety. They are available for purchase and distribution to your cardholders as a statement insert, lobby flyer or in new account kits.

Fraud and Identity Theft Statement Inserts

These inserts provide information to help your cardholders safeguard their identity and protect their financial assets from fraud. They are available for purchase and distribution to your cardholders as a statement insert, lobby flyer or in new account kits.

ATM & Debit Card Safety Tips Card Protectors

Card protectors featuring ATM and Debit Card Safety Tips are available for purchase and distribution to your cardholders.

ATM & Debit Card Safety Web Brochure for Online Statements

Provide a link to the electronic version of the ATM & Debit Card Safety insert with your online statements. This Web-based brochure is provided free of charge.

Fraud and Identity Theft Web Brochure for Online Statements

Provide a link to the electronic version of the Fraud and Identity Theft insert with your online statements. This Web-based brochure is also provided free of charge.

Safety Tips Web Site Link

Link your homepage to PULSE's ATM/Debit Safety page by using the specially designed link button. This button is provided free of charge.

If you have any questions about the Web site registration process, please e-mail webmaster@pulse-eft.com or call Ralynn Bowden at 800-420-2122.

PULSE Conducts Participant Survey (continued from page 1)

Also ranking above 9.0 were providing revenue for switched transactions, the cost of PULSE services and the responsiveness of network staff.

Although survey participants gave PULSE high effectiveness ratings in most of these categories, two areas identified for enhancements are:

- **Protection from fraud.** In the past year, PULSE introduced CVV/CVC Checking and Authorization Blocking – new fraud mitigation services aimed at increasing protection against phishing-related fraud. These are widely considered to be two of the most effective methods for combating fraud on debit transactions, and many survey respondents believe that receiving these services from PULSE has been extremely beneficial in their fight against fraud. PULSE is also in the process of implementing fraud solutions such as network-wide transaction message encryption and neural network fraud detection.
- **Revenue generation.** On April 1, PULSE implemented changes to its PIN debit pricing structure that are anticipated to increase average PIN debit interchange revenue for PULSE financial institution participants by nearly 8 percent. (The actual increase for each participant will vary depending on the mix of merchants its cardholders patronize.)

Effective Communications

The survey also addressed PULSE's value-added services, such as network communications. When asked how PULSE could better communicate with its participants, nearly 80 percent of respondents either said PULSE provides good communications currently or offered no suggestions for improvement. The suggestion cited most often was to communicate with network participants via e-mail.

PULSE has already acted on this feedback and has begun using e-mail to distribute important communications to key network contacts, when possible.

"This is just one of the ways we are applying the results of the survey," said Ballard. "We also received feedback on our performance in areas such as Web site usefulness, customer service and advertising that we will utilize to improve our performance and enhance our services in the year ahead."

1301 McKinney, Suite 2500
Houston, TX 77010

RETURN SERVICE REQUESTED

PRESORTED
FIRST CLASS
U.S. POSTAGE
PAID
HOUSTON, TX
PERMIT NO. 173

PULSATIONS **is produced bi-monthly by PULSE.**
Please send information for the newsletter to:
Casey Robinson, *PULSATIONS* Editor
PULSE EFT Association LP
1301 McKinney, Suite 2500
Houston, TX 77010
crobinson@pulse-eft.com
PULSATIONS **is posted on the PULSE Web site at www.pulse-eft.com.**