PULSATIONS

pulse®
Bringing Value to Electronic Payments®

# PULSE to Launch Fraud Detection System

## System Uses Industry-Leading Neural Network Technology to Monitor Transactions

PULSE is responding to recent growth in debit card fraud by undertaking a major initiative to help participants fight fraud. The PULSE fraud detection system, part of an enterprise-wide project in conjunction with Discover® Network, utilizes a neural network-based model to monitor and score PIN, PINless and signature transactions processed through the PULSE network.

**"We have been receiving alerts for only three days, and we have already saved thousands of dollars from possible fraud."**

**Pilot participant in PULSE's fraud detection system**

PULSE's fraud detection system is designed to help financial institution participants who are not only faced with monetary losses caused by fraud and identity theft, but are also concerned about losing cardholder confidence if a generalized incident occurs.

### Neural Networks

A neural model uses historical transaction data to "learn" about fraudulent behaviors and identify transaction activity that is either out of the ordinary for the cardholder or consistent with known fraudulent behaviors. The PULSE fraud detection system utilizes a neural network data model to monitor transactions and produce fraud authorization scores and reason codes.

When fully implemented, the system will identify suspicious transactions as those exceeding a pre-set score value and will notify financial institutions via an e-mail alert. The system is designed to help financial institutions:

- Respond more quickly to possible debit card fraud
- Reduce fraud losses
- Reduce the inconvenience of fraud to cardholders
- Decrease the loss of account holders due to fraud events

While third-party neural network services currently available often do not score PIN-based transactions, PULSE's system will be customized to detect PIN-based fraud – a critical need in the industry today.

"It is PULSE's goal to offer our participants the best available technologies for combating fraud on all transaction types," said Warren Coles, PULSE executive vice president and chief operating officer. "This service enables us to provide state-of-the-art fraud detection that will benefit all network participants."

The system is currently being tested with a pilot program involving 14 PULSE network financial institutions. PULSE plans to roll out the near-real-time fraud detection system to all participants in the third quarter of this year. By the end of the fourth quarter, PULSE expects to support automatic blocking of suspect transactions based on rules and parameters established by the card issuer.

### Rules Requirements

Special requirements for financial institution participants regarding the fraud detection system are outlined in the new *PULSE Operating Rules and Procedures*, effective August 1, 2007.

Critical to the success of the system will be fraud reporting by the issuers themselves or by issuer processors on their

(continued on page 7)


# Four-Part Series Offers Debit Fraud Prevention & Security Recommendations

As part of its commitment to provide participating financial institutions with the latest information on EFT trends, PULSE has developed the new Debit Fraud Prevention & Security Webinar Series. This four-part series will begin in September and cover current industry liability and security issues. The sessions will offer participants valuable tips and suggestions relative to:

- Debit card disputes and investigations
- Back-office scams
- Combating fraud

Two options are available for participating in this series: attend all four sessions for a discounted rate of $300 or attend individual sessions for $100 per session. Each session begins at 1:00 p.m., CDT, and lasts one hour. Registered financial institutions will receive a copy of the presentation via e-mail and an on-demand replay link to use for internal training purposes.

Detailed information on this series, including a biography of each speaker, is available on the PULSE Web site at www.pulse-eft.com/fraudprevention.html. Registration information will be mailed to all PULSE participants.

For more information, contact Melissa Voelkner at 800-282-8963 or mvoelkner@pulse-eft.com.

(continued on page 5)

*Dave Schneider*

**"We are working diligently to establish PULSE as the industry leader in electronic payment fraud detection and prevention. Our new system marks a major step toward this goal. We believe this 'intelligent' tool will assist you in adapting to ever-changing criminal strategies and tactics to commit fraud."**

Dear PULSE Participant,

Debit fraud used to be limited to lost or stolen cards, but not anymore. As debit card use has increased in recent years, so too has debit fraud. While the financial industry strives to find solutions to combat fraud, the fraudsters continue to find new ways to wreak havoc on consumers, merchants and financial institutions alike.

If you are like me, you are tired of hearing about debit fraud and ready to do something about it.

So how can you protect cardholders' financial information while reducing fraud losses? How can you get better information from cardholders, including their travel habits and spending patterns, without alienating them? How can you respond faster to possible fraud losses?

In the January/February 2007 issue of *PULSATIONS,* I revealed that PULSE had begun implementing a new fraud detection system using neural network technology. The system promises to boost your institution's fraud detection capabilities and reduce losses due to fraudulent debit transactions. As highlighted in the lead article of this issue of *PULSATIONS,* our new fraud detection system will be made available to all PULSE participants in the third quarter of 2007. The service will be free of charge to participants for the remainder of the year.

Because debit customers use their cards differently than credit card customers, our neural network-based system employs a highly customized data model developed especially for PULSE. Financial institutions large and small will benefit greatly from the service – the first of its kind implemented at the EFT network level. The system will analyze and score all transactions on the PULSE network and notify users via e-mail of possible fraudulent transactions on a 24/7 basis.

I recently sent a letter to your institution requesting you to designate two authorized system users to view and act upon fraud alerts for your institution. It is vital that all PULSE participants take part in the service so that all institutions receive the greatest possible benefit. The more feedback we get, the "smarter" the system will become.

We are working diligently to establish PULSE as the industry leader in electronic payment fraud detection and prevention. Our new system marks a major step toward this goal. We believe this "intelligent" tool will assist you in adapting to ever-changing criminal strategies and tactics to commit fraud.

Thanks for your support of the PULSE debit network.

Sincerely,

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.

### Debit Card Profitability Webinar Series

**October 2007**

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 learn about 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 debit cards and understand costs. Participants also will gain an understanding of debit cardholder demographics, as well as how cardholders respond to various debit card features.

### PIX² Advanced Web Conference

**Thursday, November 15**

This training will provide an in-depth look at the functionalities of the PIX² system. Attendees will learn more about item processing procedures and batch input/output procedures. Detailed descriptions of PIX² settlement reports also will be reviewed. This Web conference is provided to all PIX² participants at no cost.

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


Q&A

## ¿Habla Español?

**Q: What growth opportunities exist in the financial services industry?**

**A: The U.S. Census Bureau projects a 40 percent surge in the Hispanic population by the year 2020. The buying power of this group will soar nearly 48 percent between 2005 and 2010.* Is your financial institution ready?**

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

*Source: University of Georgia Selig Center for Economic Growth

*Second in two-part series*

# Data Security Best Practices

## Business Continuity and Cardholder Education Play Key Roles


Data security efforts and technologies have become part of everyday life for financial institutions. In light of the growing focus on information security and fraud prevention, PULSE has developed a compendium of tips and best practices recommended by security experts and utilized by financial institutions.

Part 1 of this series focused on information security policies, the online banking environment and the human element of data security. This second and final part addresses the need for prevention and response strategies, as well as account holder education.

### Prevention and Response

Federal Financial Institutions Examination Council (FFIEC) regulations require financial institutions to have a comprehensive business continuity plan in place to mitigate the risk of service disruptions. Financial institutions also are required to review and update their plans periodically to reflect changes in systems, software, service providers and other business details.

In March 2005, the federal financial regulatory agencies issued the "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." The guidance states that, at a minimum, response programs should contain procedures for:

- Assessing the nature and scope of an incident and identifying what systems and information types have been accessed or misused
- Notifying the institution's primary federal regulator as soon as an incident involving unauthorized access to, or use of sensitive customer information occurs
- Filing a timely Suspicious Activity Report (SAR) whenever federal criminal violations require immediate attention, and promptly notifying law enforcement authorities
- Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information
- Notifying account holders when warranted

Financial institutions that have not already done so are encouraged to form an incident response team to prepare for data compromises. It is important to develop plans for communicating with account holders, vendors, regulators – even the media, if it becomes necessary.

**TIP: If a financial institution suspects debit or credit card data has been compromised due to a hacking at a third party, the following steps can be taken:**

- Retain a professional computer forensics firm to assess the situation
- Establish a cooperative exchange with the compromised party
- Identify the population of exposed accounts/cards and consider whether notification is appropriate
- Assess the risk to the impacted accounts/cards
- Determine if the impacted cards will be reissued or replaced
- Consider the consequences of the chosen strategy (customer impact, risk of additional fraud, etc.)

### Phishing Prevention

One of the most common types of fraud is the capturing of sensitive information online. The U.S. Department of the Treasury has outlined measures financial institutions can use to prevent account holders from falling victim to such phishing attacks, including:

- Personalizing e-mails to account holders so that they can be assured of their validity
- Keeping Web site certificates up to date so that consumers can confirm the site's legitimacy
- Reminding account holders to regularly install security patches for their operating system and/or Web browser
- Posting information on your Web site directing account holders where to call to verify requests via e-mail
- Registering domain names similar to your organization's so account holders do not confuse those sites with yours
- Establishing a trademark for the domain name of the firm

If your Web site is "spoofed," the Treasury Department suggests that you:

- Immediately post an alert in a prominent place on the site describing the incident
- Monitor for unusual transaction activity
- Advise account holders who have responded to the attack to change their passwords immediately

**TIP: To assist in detecting and responding to phishing incidents, consider hiring an outside company that specializes in identifying such incidents and shutting down phishing sites.**

### Consumer Education

One of the most important aspects of data security – account holder education – also is an effective preventive measure. PULSE recommends that all financial institutions offer account holders educational materials, both in print and online, explaining key aspects of data security and outlining basic principles and precautions that account holders should take to safeguard their personal information. Such materials should address:

- Maintaining PIN secrecy
- Using strong passwords on all accounts and changing them at least quarterly
- Reviewing account statements frequently
- Changing debit and/or credit card PINs periodically
- Shredding personal documents
- Reviewing your credit report annually
- Refraining from responding to unsolicited e-mails or telephone requests for personal information
- Removing mail from mailboxes promptly
- Reporting lost/stolen cards or unauthorized transactions immediately

If identity theft is suspected, the Federal Trade Commission and Department of Justice Web sites offer a wealth of information for consumers. Consumers also have the ability to place a "fraud alert" on their credit reports to help prevent unauthorized individuals from opening an account in their name. For more information, contact the major credit reporting agencies.

### Conclusion

Enhancing the security of sensitive customer data is critical for financial institutions, and the financial services industry as a whole. The financial system is only as secure as its weakest link, and every participant in the system plays an important role – including consumers.

Financial institutions should adopt security best practices and inform account holders of the importance of adopting secure practices with regard to their personal information and finances. Collectively, these efforts will make the system stronger and increase consumer confidence in electronic payments.

# Instant Card Issuance Comes of Age

You just approved a request for a new or replacement debit card. All your customer or member has to do now is wait for their card to arrive in the mail. In the meantime, you are losing potential revenue while your cardholder loses patience. With instant issuance technology, the waiting game is over.

Instant issuance technology has been available since the late 1990s, according to Noe Rodriquez, chief information officer for Dallas-based Custom Card Systems, Inc., a supplier of instant issuance solutions. "Credit unions were the earliest to adopt instant card activation systems, but we began seeing more interest from banks about two years ago.

Today, financial institutions of all sizes and types are finding that the ability to instantly issue payments cards has advantages for both the consumer and the institution."

Rodriquez's comments are supported by PULSE's *2005 Debit Card Fraud and Benchmarking Study,* which indicated that financial institutions were looking to instant issuance to improve debit card penetration on deposit accounts. In the follow up to that study, the *2007 PULSE Debit Issuer Study,* instant issuance was also touted as a means of quickly reissuing debit cards in the event of an isolated fraud event or a large-scale data breach.

"Our cards were inactive for about a week, which made some of our members mad," noted one credit union survey respondent.

### Instant Benefits

Instant issuance, or instant activation as it is sometimes called, enables financial institutions to issue personalized debit, ATM, stored-value or credit cards from virtually any location in a matter of minutes. This affordable technology delivers a number of benefits to financial institutions:

- Eliminates the time, expense and risk associated with sending personalized cards through the mail
- Promotes immediate use of payments products to generate revenue right away
- Enables on-site training of cardholders
- Creates a prime opportunity to mention other products and services
- Demonstrates commitment to customer service and satisfaction

"Instant issuance is easy to use and our members love the convenience," stated Holly Walker, card services manager at Credit Union of Texas, which has employed the technology since the fall of 2002. "We enter the card request into the core processing system. The member then picks a personal identification number and enters it onto a PIN pad. The request is sent to the embossing machine, which puts the member's name and card number on the card, along with the required encryption. The entire process takes less than two minutes."

David Weems, vice president at First Technology Services, the processing arm of First Financial Bankshares, a holding company for nine Texas banks, began using instant issuance in early 2006. They now have more than 40 branches with instant issuance capabilities. He summed up the advantages of the technology this way: "Instant issuance is a win-win for our banks and for our customers. They like the speed and convenience of the technology. We like the fact that they can begin using their cards right away."

Rodriquez noted that the hardware and software required for instant issuance costs about $10,000 per branch. The typical embossing machine is about the size of a large desktop printer. For more information on instant issuance, contact the Debit Solutions Client Support Team at 866-203-8760 or via e-mail at debit_solutions@pulse-eft.com.

# Pennsylvania Bank Joins PULSE

## Adams County National Bank to Issue Discover® Debit

Adams County National Bank, a financial institution serving south-central Pennsylvania for 150 years, has signed a long-term agreement with PULSE for debit card transaction switching and settlement.

The bank, which has 21 branches, is utilizing PULSE exclusively for PIN debit purchases and will introduce a Discover® Debit program, offering the signature debit card to selected customers. Adams County National Bank also utilizes PULSE for ATM transactions.

"In addition to utilizing PULSE exclusively for PIN debit transactions, we plan to issue the Discover Debit consumer card to a targeted group of existing cardholders who currently have PIN-only cards, giving these customers a product that features greater functionality than their current cards," said Lynda L. Glass, executive vice president and chief operating officer of Adams County National Bank.

"We are proud to have been selected by Adams County National Bank to meet its growing electronic payment needs," said Leah Henderson, PULSE executive vice president. "For PULSE, signing an exclusive PIN debit agreement with a Pennsylvania bank confirms that financial institutions in diverse areas of the country recognize the national reach of the PULSE network."

PULSE is continuing to make progress with regard to financial institution participation, as demonstrated by the 21 percent transaction growth the network reported in the first half of 2007, compared to the first half of 2006.

"In particular, we are pleased with the results of our efforts in the Southeast and Northeast regions of the U.S.," said Henderson.

## Four-Part Series Offers Debit Fraud Prevention & Security Recommendations (continued from page 1)

### Debit Card Disputes and Investigations

**September 11 and 13**
**Andrew Paur, Esq.**

Financial institutions face a complex set of laws, rules and regulations in connection with their debit card programs. A review of the legal requirements that apply to financial institutions that issue debit cards will be presented in this session. Important considerations relating to debit card disputes and investigations, such as those arising from the Electronic Funds Transfer Act (EFTA), Regulation E, common law and card association bylaws and rules will be highlighted.

### Back-office Scams

**September 18**
**Gregg Bennett, President of Pivotal Financial Resources**

This session will cover common scams and fraudulent activities that occur in the back offices of financial institutions. Forgery, counterfeiting, kiting, unauthorized transactions and ATM fraud are among the topics that will be addressed. Participants also will learn about protection methods to help decrease fraudulent activity within their institutions.

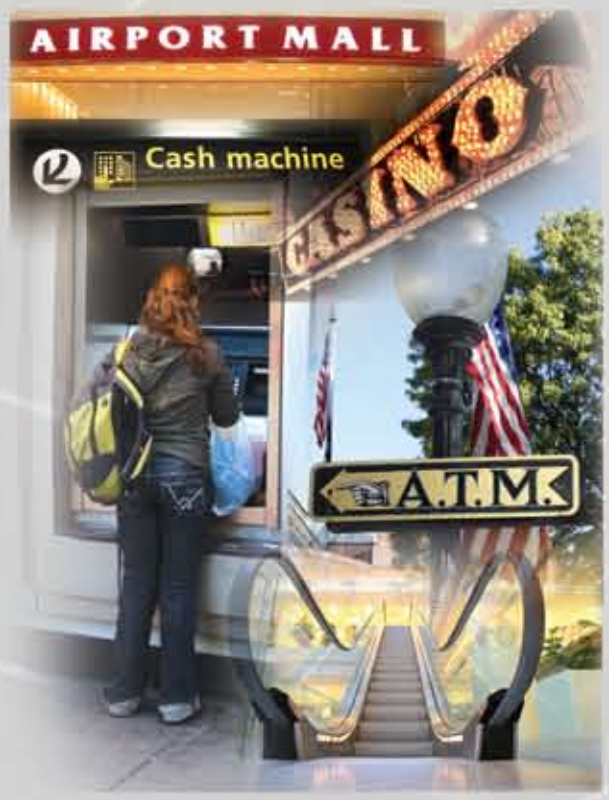
### Fighting Back Against Fraud

**September 25**
**Robert Rebhan, Former Detective Sergeant with the Los Angeles Police Department**

This presentation will provide insights into current fraud trends, and measures that financial institutions can take to combat fraud. The most up-to-date fraud and identity theft schemes, as well as practical advice on how individuals and businesses alike can avoid becoming victims of these crimes, will be discussed.

# Cutting Ties

## Issuers Deploy Wireless Technology for Off-Premise ATMs




Financial institutions are increasingly implementing wireless telecommunications technology on their off-site ATMs. The benefits of the technology include increased flexibility and reduced monthly operating expenses.

Wireline-connected ATMs are limited in terms of where they can be placed, due to their use of the telecommunications infrastructure. And in today's climate of highly compressed ATM margins, deployers can benefit from the additional flexibility provided by wireless connections.

The use of wireless technology enables financial institutions and other ATM owners to optimize the placement of their machines and thereby maximize traffic. Wireless ATMs also can be redeployed to new locations easily and inexpensively, as traffic patterns change.

Memphis-based First Tennessee Bank, a PULSE participant since 1997, has converted approximately 315 of its off-premise dial-up ATMs to wireless technology. The driving force behind this decision was a significant reduction in monthly operating expenses, said Michael Marzec, a senior vice president with First Tennessee and a member of the PULSE Financial Institution Oversight Committee.

"In addition, because the ATMs are continuously connected by wireless telecom, we have full monitoring capabilities," Marzec said.

The implementation of wireless technology has enabled First Tennessee to reduce transaction times from the 55 seconds that was typical with dial-up modems to about 35 seconds. And the time required to download new screens and software updates, for example, is now about five minutes, compared to 20 minutes prior to deployment of the new technology.

Because the data from a wireless ATM travels over the public airwaves, there are special security considerations that must be employed with the technology. Marzec said First Tennessee uses Triple-DES encryption on the entire transaction message – not just the PIN. There also are off-premise locations where wireless machines are not the optimal solution, such as areas with low or no cellular coverage or hospitals, where cell phone use is prohibited.

Are wireless ATMs the wave of the future? That remains to be seen, but as a result of the increased flexibility they provide, as well as reduced installation costs, rapid deployment and enhanced connectivity, ATM deployers are expected to utilize the technology in increasing numbers in the coming years.

# GAO Study Explores Data Breaches and ID Theft

**"An expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether."**

**United States Government Accountability Office**

In response to a request by Congress, which is considering legislation to establish a national requirement for data breach notifications, the United States Government Accountability Office (GAO) has analyzed data breaches that have occurred in the U.S., as well as the resulting fraud.

Specifically, the GAO was asked to examine the incidence and circumstances of data breaches, the extent to which they have resulted in identity theft, and the potential costs, benefits and challenges of enacting notification requirements.

More than 570 separate data breaches were reported by the news media in 2005 and 2006, according to the GAO. These incidents varied widely in terms of size and occurred at organizations ranging from merchants and financial institutions to government agencies, universities and medical facilities.

Because it is difficult to directly link fraudulent activity with the point of compromise, in addition to reviewing the available data, the GAO conducted interviews with researchers, law enforcement officials and industry representatives. Their conclusion was that most data breaches have not resulted in identity theft, and particularly not in the unauthorized establishment of accounts in victims' names.

Of the 24 largest breaches that occurred between January 2000 and June 2005, only three breaches can be linked directly to fraud on existing accounts, and only one to the unauthorized creation of a new account.

"Requiring affected consumers to be notified of a data breach may encourage better security practices and help mitigate potential harm, but it also presents certain costs and challenges," said the GAO in a report on the study. "An expansive requirement could result in notification of breaches that present little or no risk, perhaps leading consumers to disregard notices altogether."

Federal banking regulators have advocated a risk-based notification standard, as has President Bush's Identity Theft Task Force. The GAO report concludes that, "Should Congress choose to enact a federal notification requirement, use of such a risk-based standard could avoid undue burden on organizations and unnecessary and counterproductive notifications of breaches that present little risk."

To view the full GAO study, visit www.gao.gov/new.items/d07737.pdf.

# UMB Selects PULSE as Exclusive PIN Debit Network

UMB Financial Corporation, a PULSE participant since 2003, has elected to extend and expand its relationship with the network through a long-term agreement that establishes PULSE as the sole provider of PIN debit network services to the company.

An $8 billion multi-bank holding company headquartered in Kansas City, Missouri, UMB provides a broad range of banking and financial-related services to consumer and business customers. UMB banking subsidiaries own and operate 138 banking centers throughout Missouri, Kansas, Illinois, Colorado, Oklahoma, Nebraska and Arizona.

George Schmelzel, senior vice president of UMB Card Services, said the new agreement with PULSE will further the bank's growth in a rapidly evolving debit marketplace.

"We are committed to providing unparalleled customer service, and to creating an environment that consistently exceeds account holders' expectations," Schmelzel said. "UMB takes pride in having a reputation as a financial institution that anticipates our customers' needs, and we look forward to strengthening this reputation through our growing relationship with PULSE."

PULSE is pleased to have been selected by UMB to meet its growing electronic payment needs.

"As a leading electronic funds transfer network and a pioneer in developing electronic payments, we realize how important it is to provide the highest quality of service to our financial institution participants," said PULSE President Dave Schneider. "UMB's decision to utilize PULSE as its exclusive PIN debit network confirms that we are achieving this objective."

George Schmelzel also will serve on the PULSE Financial Institution Oversight Committee. Created in 2005, the committee advises PULSE on key issues regarding the network.

# Business Continuity – the Importance of a Flexible Plan


One of the concurrent sessions at the 2007 PULSE Conference was titled *Never Gamble with Your Business Continuity Program,* and was presented by Alice Staten with Discover Financial Services and Elizabeth Hale with CC Pace. Staten raised an important question to financial institutions considering modifying their business continuity plan: Just how high are the stakes if you don't have a feasible, executable plan?

Staten stressed the importance of the payments industry to consumers using Discover Financial Services as an example. There were more than three billion payments transactions processed by just the Discover Network and PULSE in 2006. These payments affected merchants and customers all over the world, and included critical bills such as home loans, auto loans and payments for utilities, groceries and gasoline. The payments industry affects people at home, at work and while traveling, and protecting this industry in times of disaster is paramount to community disaster recovery.

Like many companies, Discover started its planning efforts in the mid-1990s, when Y2K fears heightened awareness of the need for continuity planning in industries around the world. Discover needed a design that would encompass many business units under one plan. The company implemented an annual evaluation of their business units and established a team of continuity planners to help develop and document the individual plans, which they wanted to bring together into one major plan. Discover believed a plan that was flexible and would allow for continuous improvement would best serve their needs. Discover's overall mission was to concentrate on life safety, as well as business recovery.

Key to the plan's success was buy-in from Discover management. The planners used a software package that provided a consistent methodology across business units. The business units outlined narratives, identified tasks and critical processes, assigned teams and completed call list rehearsals. In the end, an effective overall business continuity plan (BCP) emerged in 2005 – one that reflected Discover's corporate strategy and established rapid notification and employee information systems.

It was important to not only identify, but also prioritize critical processes, based on their overall business impact. Risk assessments by location were conducted. Vendor surveys were implemented. Training for continuity teams was developed and rehearsals were conducted for different business areas.

Discover has continued to refine its BCP. New scenarios have been added to include weather-related disasters and pandemics. The goal is a strategy that is workable for up to 80 percent of incidents, and the flexibility to allow for cooperation with assistance groups or help with humanitarian efforts. Discover will continue to improve its BCP, always with careful consideration of the human element, because, ultimately, there is no business if there are no people there to run it.

Hale stressed the importance of considering not only disasters, but also supplier outages and government interruptions. She provided some critical elements of a BCP, including:

- A strongly stated, enterprise-wide statement of policies and procedures
- A clear definition of responsibility
- Detailed internal and external communication plans
- A prioritized list of critical activities
- Emergency mitigation strategies
- Clear direction for the emergency management team and sub-teams
- Enterprise-wide training that includes well-conceived test scenarios
- Careful documentation of everything

Both speakers stressed the importance of working with outside groups such as local, state and federal agencies where feasible, and building in continual plan updates. A BCP is a living document and needs to be continually evaluated in order to maintain its effectiveness. The stakes to both the company and its customers are too high to take a chance with its BCP.

## PULSE to Launch Fraud Detection System (continued from page 1)

behalf. The new rule set requires each issuer to register two representatives as system users who can be contacted to review suspicious transactions.

PULSE has sent letters to all participating institutions to request their two system user contacts, and has provided details on how these contacts will register to receive e-mail alerts and view suspect transactions. Online training is available for the users so they can learn how to use the service, manage fraud alerts and submit their institution's confirmed fraud. To register for the next PULSE Fraud Detection System Webinar, or to listen to a previously recorded session, visit www.pulse-eft.com/pulsesecurity.

"It is important that every PULSE network participant take part in the system in order for all institutions to receive the greatest possible benefit. This particular initiative is a direct response to what we know is a growing concern of financial institutions – fraud risk," said Dave Schneider, PULSE president.

### How It Works

Debit transactions are scored by the neural model and, if the assigned score is over the preset limit, an alert is e-mailed to system users for the financial institution involved. Users can log into a secure PULSE Web site to view the transactions in question. Upon review, users may classify the suspect transactions as "Fraud" or "Not Fraud," based on their institution's investigation, then determine the next course of action, depending on the institution's fraud mitigation policy. This information, along with confirmed fraud submitted to PULSE on a monthly basis, is being used to enhance the neural model and improve its accuracy.

In 2007, alerts will be provided in near real-time. System enhancements will be announced in 2008.

There will be no charge for the service in 2007.

Pilot program participants already have been experiencing the benefits of the fraud detection system. "We have been receiving alerts for only three days, and we have already saved thousands of dollars from possible fraud," said an executive from a regional financial institution at a recent user group meeting, hosted by PULSE.

### PULSE's Fraud Detection System

- **Detects fraud and identifies suspicious card activity using neural network technology**
- **Generates unique score and reason codes for each transaction**
- **Monitors transaction score thresholds and issues alerts to financial institutions**
- **Becomes more proficient at identifying suspicious or fraudulent transactions with confirmed fraud submitted by financial institutions**

*For more information about the PULSE fraud detection system, visit the PULSE Web site at www.pulse-eft.com/pulsesecurity, or contact PULSE at 800-420-2122.*

# IN CLOSING...


## PULSE Sponsors CSBS Golf Outing

In May 2007, PULSE sponsored the Annual Conference of State Bank Supervisors (CSBS) Golf Outing for the sixth consecutive year. Pictured with Warren Coles, PULSE executive vice president and chief operating officer (middle), are Neil Milner, CSBS president and chief executive officer (left) and Jeffrey Vogel, chairman of CSBS (right).

## Regulation E Requirement Change

On June 28, 2007, the Federal Reserve Board announced its approval of the rule to create an exception for transactions of $15 or less from the Regulation E requirement that receipts be offered to consumers for transactions initiated at an electronic terminal. This rule will make it possible for consumers to use their debit cards in retail situations where offering receipts may not be cost effective or practical.

For more information on this rule, visit the Federal Reserve System's Web site at www.federalreserve.gov.

## Mark Your Calendar for the 2008 PULSE® CONFERENCE

**April 28-30 Wynn Las Vegas**

Join us for the 2008 PULSE Conference, ***P3 – Protect, Perform, Profit.*** Together, we will explore new frontiers in fraud prevention, examine best-in-class performance practices and discuss proven strategies for maximizing debit profitability. You'll also enjoy a pre-conference workshop, golf, ample networking opportunities and Las Vegas-style entertainment. Focused general and concurrent sessions presented by nationally recognized speakers will deliver everything needed to maximize the full potential of your debit programs.

PERFORM
PROTECT P3 PROFIT

pulse®

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.**