Partner with the Bank to Combat Constant Payments-Fraud Threat

Remote Deposit:
From Infancy to Adolescence

SinglePoint® Alerts Messaging:
Let Banking Information Chase You
Partner with the Bank to Combat Constant Payments-Fraud Threat

In the struggle against payments fraud, the rising number of fraud attempts remains constant. Criminals get more innovative every day. And the best way to protect your business against losses? Nothing new there either — it’s still partnering with your bank and using appropriate fraud-prevention tools.

The most recent Association for Financial Professionals (AFP) Payments Fraud Survey confirms that payments fraud remains a major challenge to the business community. In the 2007 survey, 72% of companies reported attempted or actual payments fraud in the previous year, and 39% said incidents of fraud increased over the previous year.

Why should companies care? Since the early 1990s, the Uniform Commercial Code has said that a company — and not its bank — must bear liability for check fraud losses if the company was in the best position to prevent the fraud but didn’t.

Put another way: If your bank offers you a fraud prevention tool and you refuse it, and then you get hit with a large-dollar fraud that the tool could have prevented, your company could bear the greater liability for the loss.

“The bank has a key role in offering fraud-prevention products, but the customer must act as a partner in fraud-prevention efforts,” says Steven Helgen, a Vice President in Commercial Product Management at U.S. Bank.

Check fraud: top threat
Check fraud remains the top payments fraud threat, according to the AFP survey, as nearly all organizations that reported payments fraud said they were victims of check fraud. The most prevalent forms reported in the survey were:

- Altered payee names (61%)
- Counterfeit checks that had the organization’s own MICR line but used another organization’s name (57%)
- Lost, stolen or counterfeit employee paychecks (41%)

Helgen says he’s also seen rising fraud related to pre-authorized drafts, which don’t require signatures. Criminals issue these drafts against legitimate business
accounts, deposit them into their own accounts, drain those accounts and disappear, he says.

**Check-fraud prevention tools**

U.S. Bank offers an array of check-fraud prevention tools, headlined by SinglePoint® Positive Pay. This convenient, state-of-the-art service is designed for companies that can transmit check-issuance information to the bank on a timely basis. “Customers have online access to images of exception items and can return them directly from the SinglePoint page,” Helgen explains.

Users can upgrade to Payee Positive Pay, so that in addition to check number and amount, the bank reviews each check’s payee name against issuance data.

Other U.S. Bank check-fraud prevention tools include Reverse Positive Pay (the bank sends check presentment data to the company for matching) and a Check Filter service that enables companies to set dollar limits on checks paid from a particular account or prevent checks from posting to an account at all, if the account is used only for depository activity.

**ACH fraud: No. 2 and climbing**

A little more than one-third of the companies reporting an attempted or actual fraud in the AFP survey experienced Automated Clearing House (ACH) debit fraud. Helgen says ACH debit fraud is growing and dangerous.

“We’ve noted more individual consumers creating fraudulent debits against business accounts,” he says. "Many cases involve credit card payments where the account ownership is not verified by the credit card company. We’ve also seen cases of social engineering where businesses were duped, either through phone calls or emails, into directing their invoice payments to a different bank account.”

**Thwarting ACH crime**

U.S. Bank also offers many tools designed to curb ACH fraud.

“The newest one is ACH Positive Pay, which allows a business customer to review received ACH debits each day and make pay/no pay decisions, very much like Reverse Positive Pay on the check side,” Helgen says.

Other tools include an ACH Block, which allows you to prohibit any ACH debits against a particular account or accounts; an ACH Filter, which enables you to designate which company or companies can debit a particular account; and Universal Payment Identification Codes (UPICs), unique bank account identifiers that allow businesses to receive electronic payments without divulging their banking information.

To learn more about any of these tools, as well as other helpful fraud-prevention best practices, contact your Treasury Management Sales Consultant.
Remote Deposit: From Infancy to Adolescence

Among the first banks to offer a remote deposit solution, U.S. Bank launched U.S. Bank On-Site Electronic Deposit in September 2004, providing the check-scanning equipment and PC software customers needed to scan and deposit checks electronically, as well as the technology to convert paper checks into Automated Clearing House (ACH) credits. Over the past four years, remote deposit has become an increasingly popular cash management tool offered by banks — big and small.

As technology progresses and develops, and processes are refined and perfected, remote deposit solutions continue to offer customers higher levels of convenience and efficiency. The following article highlights some of the major milestones in the development of remote deposit solutions and provides a look into what lies ahead.

The journey from Check 21 to image exchange

By facilitating truncation of the physical check, the Check Clearing for the 21st Century Act, also known as Check 21, quickly led banks to develop remote deposit products, such as On-Site Electronic Deposit, and launched new check-clearing efficiencies. Companies implementing remote deposit services quickly realized the convenience of no longer being bound to the business hours of their local bank branches to make daily deposits, as well as the time and cost savings of not having to make trips to the bank or hire a courier service. In addition, companies were able to consolidate their banking relationships, as they were no longer limited to the bank’s traditional branch footprint.

Although banks provided the ability to make deposits electronically from an office location, substitute checks, a paper reproduction of the original paper check covered under Check 21, continued to be the norm in item processing. To realize the full potential of remote deposit, and the vision of a paperless check-clearing system, banks set out to implement image exchange, a process by which U.S. financial institutions can receive and send check images.

Today, a handful of banks, including U.S. Bank, are beginning to migrate remote deposit products to an image exchange platform. While only a few banks are currently equipped to use image exchange, more and
more are expected to get on board as the image exchange network develops and grows. As a result, the efficiency of clearing checks will continue to increase.

The next generation of remote deposit
When On-Site Electronic Deposit was first launched, all data from checks and remittance documents was manually entered into the system. In 2006, Courtesy Amount Recognition (CAR) and Legal Amount Recognition (LAR) software was added to provide a mechanism for customers to reduce deposit preparation and processing time. CAR/LAR technology automatically populates the dollar amount of the check, decreasing the amount of time it takes to enter data.

The emergence of browser-based applications has provided customers a more efficient method of implementing remote deposit. In early 2007, U.S. Bank launched a Web-based version called On-Site Electronic Deposit Web, which simplifies the deployment process by eliminating the hassles associated with software installation and upgrades. Customers with multiple locations or limited resources for desktop technical support welcomed the simplicity of Web-based access.

As a streamlined alternative to the original PC-based service, On-Site Electronic Deposit Web offers new workflow tools through a centralized dashboard, enabling companies to customize controls for the scanning, data entry, balancing and approval process. This optional segregation of duties functionality allows for more efficient processing and monitoring of the transaction process.

Looking ahead
In 2008, On-Site Electronic Deposit Web will be integrated into U.S. Bank SinglePoint®, U.S. Bank’s online treasury management services Web portal. Customers will be able to access OED Web and the Electronic Deposit Manager, an image search and reporting tool, through a single sign-on process. Integration with SinglePoint will eliminate the need for customers to maintain multiple passwords while adding another level of security.

The convergence of electronic check-clearing alternatives such as substitute check, image exchange and ACH conversion has led to new reconciliation processes and challenges for customers. In 2008, to simplify the end-of-day reconciliation process, U.S. Bank will streamline deposit reporting by providing a single, daily credit for all image check and ACH deposits processed through On-Site Electronic Deposit. This new process will enable customers to quickly and easily reconcile their On-Site Electronic Deposit activity totals to their bank account.

Looking to the future, banks will continue to explore and develop new opportunities to eliminate checks from the traditional clearing process, providing business customers with faster access to funds and more efficient payment collection processes. For more information on how remote deposit can benefit your company, contact your Treasury Management Sales Consultant.
SinglePoint® Alerts Messaging:
Let Banking Information Chase You

Nobody likes to wait for important financial information. That’s why in the past treasury managers have spent many days repeatedly logging into their bank information reporting systems, each time checking to see if, for instance, any wire transfer approvals are needed, or possibly if an account balance has reached a certain threshold.

Fortunately, U.S. Bank customers now can eliminate time-consuming banking queries by using the alerts messaging capabilities of U.S. Bank SinglePoint®, our treasury management services Web portal.

By utilizing SinglePoint alerts, you no longer have to chase down important banking information. Instead, the bank sends you a message when the information is available. Over 35 different alerts are offered.

SinglePoint can deliver alerts in two ways. The first is to post messages at a customer’s SinglePoint landing page, also known as the “LaunchPoint” page.

The second method is external messaging. We email messages that you retrieve from an Internet connection, an email-enabled cell phone or other email-enabled handheld device. That way you can access banking information when you’re away from the office.

LaunchPoint alerts
LaunchPoint access to bank messages is provided at no additional cost to SinglePoint users. When you access the LaunchPoint page, it offers you four alert options:

- **Bank messages.** These can relate to any important event the bank needs to report, such as a service outage or a new product release.

- **User tasks.** Messages under this heading include information the receiver must act upon, such as a wire transfer needing approval or a Positive Pay exception item requiring a “pay” or “no pay” decision.

- **User messages.** These are other messages related to U.S. Bank treasury management services, such as a notice that a DDA statement or a lockbox report has become available.
What’s new. Here’s where you can access details of new products and other bank news, including new editions of the TM Forum eNewsletter.

Save time, increase productivity
SinglePoint offers alerts related to all of the bank’s treasury management services, saving you time across a range of banking activities. “We will continue to add alerts each time we introduce a new functionality to SinglePoint,” adds Elizabeth Eidsmoe, a SinglePoint Product Manager.

There are even alerts that support system administration, she says.

“Let’s say you’re a system administrator and are responsible for approving new users or user modifications,” Eidsmoe explains. “You can receive an email alert on your cell phone to let you know that a user is waiting approval. So even when you’re traveling you can log in to review those user changes.”

Receive messages at multiple locations
SinglePoint users can have alerts sent to multiple locations. You can have messages sent to your LaunchPoint page, to any number of email addresses if you use external messaging, or to both LaunchPoint and email addresses.

The external messaging service requires a $25 monthly maintenance fee, but there are no limits on the number of users or messages.

Customize alerts by user
Users can establish LaunchPoint alerts online without assistance. Subject to user entitlements, you can enable whichever alerts you desire and dictate where those messages should be sent.

What’s more, you can establish the frequency of your messages: immediate, every half hour or every hour.

To initiate external messaging, contact your U.S. Bank Treasury Management Sales Consultant.

Future enhancements
An alerts enhancement planned for 2008 is the ability to notify a system administrator when another administrator resets a user password.

Another planned enhancement is a message to inform system administrators of global settings changes. For instance, if initiating an ACH transaction at a company requires one approval and an administrator changes the settings to zero approvals, other system administrators would be alerted. “We think this new feature will be appreciated by customers who are tightening controls in light of the Sarbanes-Oxley Act,” Eidsmoe says.

U.S. Bank also is exploring technology that would allow external messaging recipients to act on user task messages via their cell phone or other email-enabled device (e.g., rendering a Positive Pay decision or approving a wire transfer).