

▶▶▶ Recent Economic Challenges Have Helped Accelerate Shift to Electronic Payments

Companies have been working hard to migrate from paper to electronic business-to-business (B2B) payments. One of the many factors driving this migration in recent years has been the challenging economy.

▶▶▶ Maintain Vigilance Against Online Payments Fraud as New Threats Continue to Emerge

Preventing online payments fraud remains a daunting challenge, with new threats constantly emerging, including social media related dangers and attacks on mobile phones.

▶▶▶ Remote Deposit Processes Streamline Delivery of Cash, Checks to the Bank

If your treasury staff is spending too much time making daily cash and check deposits at your local bank branch, consider innovative deposit solutions from U.S. Bank

▶▶▶ Minimize Fraud Losses Using Check Fraud Prevention Services

The statistics are staggering—payment fraud activity is increasing at a rapid rate. According to the 2010 AFP Payments Fraud and Control Survey, 73% of organizations experienced attempted or actual payment fraud in 2009.

▶▶▶ *The Power of Green* Golf and the Environment

Next time you are out on the greens, think about whether your own actions are "green." Here are some easy suggestions on what you can do to help the environment.

Recent Economic Challenges Have Helped Accelerate Shift to Electronic Payments

Spring 2011

Companies have been working hard to migrate from paper to electronic business-to-business (B2B) payments, as evidenced by the results of a national survey. One of the many factors driving this migration in recent years has been the challenging economy.

According to the 2010 Association for Financial Professionals (AFP) Electronic Payments Survey results, released late last year, the typical organization now makes 57% of its B2B payments by check. That's down from 74% in 2007 and 81% in 2004, indicating that the migration to electronic payments is accelerating.

What's more, half of the survey respondents say their organizations are very likely to convert a majority of their B2B payments to major suppliers from checks to electronic payments in the next three years.

"Many companies were working on migrating to electronic payments already, but the pressing economic environment probably helped accelerate those projects," says David Bellinger, Director for Payments at AFP. "The financial crisis forced corporations to look for efficiencies and improved cash flow, and treasury managers have seen migrating to electronic payments as one way of pursuing those goals."

Drivers and benefits

Advances in technology and an increased focus on business improvement are both major factors driving the growth of electronic B2B payments, according to the survey results.

From a technology perspective, Bellinger says companies are taking advantage of the development of new standards and SWIFT platforms that make it easier to integrate electronic payments into their



accounting systems. He says the focus on business improvement relates to a desire to both reduce hard-dollar costs, such as expenses related to printing and mailing paper checks, and achieve soft-dollar cost savings by freeing up time for treasury staffers through more streamlined work flows.

Additionally, electronic payments result in fewer exceptions to process, which can create significant time savings for treasury departments, Bellinger says. "Corporate treasury staffs have become particularly lean in recent years, and anything that buys them some additional time is valued highly."

Survey respondents cite cost savings (52%), improved cash forecasting (40%), and fraud control (37%) as the top benefits of electronic B2B payments.

Corporations began putting a major emphasis on improved cash forecasting during the recent financial crisis, Bellinger says. "They began focusing more than ever on knowing where their cash was coming from, when it would hit their books and when it was going to become available," he says. "Improved cash forecasting

Spring 2011

enables a company to plan better, get higher rates on investments and better manage its debt position, and electronic payments help provide the cash flow predictability that makes that possible.”

Overcoming barriers

According to the AFP survey, the top remaining barrier to converting to B2B electronic payments is “difficulty convincing suppliers to accept electronic payments,” which was cited by 83% of respondents. Other barriers they cited include:

- Inability of trading partners to send or receive automated remittance information with electronic payments (77% of respondents)
- No standard format for remittance information (72%)
- Shortage of IT resources for implementation (70%)

Despite these obstacles, Bellinger says he expects “slow and steady progress” in companies issuing fewer paper checks and increasing their electronic payments. Much of the new electronic payment volume will be in the form of wire transfers and Automated Clearing House (ACH) payments, he says, noting that more respondents reported integrating their accounting systems with their ACH payment systems than with their commercial card systems.

Bellinger notes that companies will continue to have the greatest success in converting to electronic payments with their major suppliers, where relationships are strongest and the companies are typically larger and share similar cost-savings goals.

However, he cautions that another factor that could slow the acceleration of the e-payment migration trend is the practical matter of limited treasury staffing.

“With corporations having such lean treasury staffs, change is necessarily limited by how much time they have to focus on special projects like electronic payments,” Bellinger says.

To learn more about U.S. Bank electronic payment products and strategies for migrating to e-payments, contact your Treasury Management Consultant.

Maintain Vigilance Against Online Payments Fraud as New Threats Continue to Emerge

Spring 2011

Preventing online payments fraud remains a daunting challenge, with new threats constantly emerging, including social media related dangers and attacks on mobile phones.

In one of the newer developments on the online fraud front, fraudsters have begun leveraging social media in cyber attacks, according to Laura Listwan, Senior Vice President-Product Development at U.S. Bank. Criminals collect information about victims and their jobs through social Web sites like Facebook, she says.

“Fraudsters use social media to get to know who you are on a more personal level, so a scam sounds even more real,” Listwan says. “Technology is changing, and the creativity of fraudsters is terrifying.”

For example, you might receive a phone call from a fraudster purporting to be one of your vendors — convincing because he seems to know all about you. The caller says his company has changed banks and he needs to send you new banking information for your next payment, Listwan says.

To make matters more challenging, today’s cyber criminals are patient as well as creative, she says. They monitor banking activity and study patterns over time, sometimes for more than a year, to give them an edge when targeting a particular computer user.

New target: mobile banking

In addition to securing computers, treasury professionals these days also need to protect their mobile phones. With the increase in mobile banking, fraud attempts through smart phones are on the rise, Listwan says. She stresses the importance of protecting smart phones in the same way you would



protect your computer. “Smart phones are mini PCs,” she says. “They have a lot of information you don’t want compromised.”

Rogue anti-spyware

When trying to defend against malicious software, known as “malware,” beware of rogue anti-spyware scams, Listwan says. In an increasingly common ploy, fraudsters will induce alerts on your computer screen alleging that your computer is infected with a virus and offering a link to anti-spyware that supposedly will cure your machine’s ills. By clicking on the link, you may end up infecting your computer with an additional, more insidious virus.

Once infected, a computer will need to be re-imaged, which requires removing all of its software and reinstalling it.

Traditional scams

In addition to all the new criminal strategies, more traditional cyber scams continue to pose an ongoing threat to online payment processing systems. For example, a treasury manager might be directed to a fraudulent Web site that captures the manager’s

Spring 2011

personal information, including IDs, passwords and wire PIN information, and then informs the user that the actual Web site is down for maintenance. Having this information gives the criminal access to online banking applications.

“To help protect against such scams, treasury managers should initiate all payment transactions under ‘dual control,’ where one individual initiates the payment and another approves it,” Listwan advises. “Setting appropriate user limits is also critical.”

Listwan also warns against accessing any Web link that you don’t recognize, and suggests even being cautious about those links that you do recognize.

Education, best practices

Educating staff plays an important part in maintaining computer security, Listwan says. Employees benefit from such education both in the workplace and at home.

Treasury managers should develop strict Internet use policies for staff involved in payment activities, and those policies should be documented, reviewed and updated as necessary, she says.

One key policy is that you should not allow access to personal e-mail and Web surfing on computers that are used for payment initiation. Additionally, you should institute a policy requiring the separation of duties for online payment related processing. The employee who initiates payments should not be allowed to reconcile those payments.

To improve overall computer systems security, Listwan also recommends the following practices:

- Maintain updated systems and software.
Configure anti-virus software (AVS) to update

regularly and scan automatically. “AVS is only as good as what it can protect you against,” she warns. If a virus is detected, it can take as long as 30 to 45 days to develop a patch, so it is important to realize that AVS alone is not enough. Also, understand which plug-ins are installed on your computer, Listwan advises, and know that they are not automatically updated when AVS is updated.

- Install a firewall between your computer and the Internet.
- Block pop-up windows that could conceal cyber attacks.
- Tighten security settings on browsers.

Finally, it is vital to use common sense when dealing with computers, and each Treasury staff member must take a personal role in fraud protection, Listwan emphasizes. “Preventing online payments fraud starts with computer software, but that only goes so far,” she says.

Remote Deposit Processes Streamline Delivery of Cash, Checks to the Bank

Spring 2011

If your treasury staff is spending too much time making daily cash and check deposits at your local bank branch, consider innovative deposit solutions from U.S. Bank. One company that has is SSP America, which implemented Remote Cash Deposit to both gain efficiency and reduce the risks associated with collecting cash at its airport restaurants and concessions.

“Cash-focused businesses like ours continually seek ways to enhance risk management and move cash quickly from employees’ hands to our bank accounts,” says Joe Scott, Treasury Specialist at the company. “Remote Cash Deposit has helped reduce our reconciliation and theft woes by calculating deposits automatically and eliminating fraud.”

Many businesses with cash receipts for services or goods are ideal candidates for Remote Cash Deposit. Customers using the service deposit cash directly into safes they lease from a national armored courier. They determine the lowest bill denomination that employees must deposit into the safe (e.g., quick-serve restaurants may establish a \$20 minimum while convenience stores select \$10).

The safe’s bill acceptor — similar to a vending machine’s — reads the bill’s amount and scans it to detect counterfeits. Once bills are deposited into the safe, only the armored courier can access them. The safe tallies deposits automatically, saving employees from counting or over-handling cash.

Customers schedule safe pickups with their armored courier, which processes and delivers cash to U.S. Bank. Prior to pickup, however, customers gain access to those funds under the following schedule. Cash is deposited into the safe on Day 1. That night or early on Day 2, the armored courier extracts data from the safe through a wireless or virtual private network connection and forwards it to U.S. Bank. In turn, the



bank credits the customer’s account on Day 2. The customer can view previous-day depository activity on the morning of Day 3 through SinglePoint®, the Web portal to U.S. Bank’s suite of treasury management services.

Deploying Remote Cash Deposit also removes sensitivities that businesses like quick-serve restaurants or retailers often have about hourly employees handling and reconciling cash they depend upon for operating cash flows.

“With new cash deposit processes in place, employees can focus on greeting customers and dispensing concessions without worrying about reconciling cash drawers at the end of their shifts,” Scott adds. “On-site managers can also focus on strategic tasks rather than micro-managing employees or agonizing over potential theft.”

The solution delivers these additional benefits:

- Depository accuracy. Remote Cash Deposit can eliminate some of the errors typically found in manually counted deposits. More accurate data means employees won’t waste time researching adjustments when counted cash and reported receipts don’t match.

Spring 2011

- Increased staff safety. Physical trips to the bank are eliminated or minimized, which reduces fraud and employees' potential of being robbed.
- Better use of staff time. Managers who once counted cash can provide value to their employees by assisting employees or customers on the store floor.

Deposit Checks Electronically

Companies can streamline the deposit process even further with U.S. Bank's On-Site Electronic Deposit, which lets them use remote deposit capture technology to electronically deposit checks from the convenience of their offices.

"On-Site Electronic Deposit eliminates manual depository processes, such as physically depositing checks at a bank branch, that take staff members away from performing strategic tasks in the office," says Stephanie Schmitt, Vice President of Global Treasury Management Product Management, U.S. Bank.

To use the product, customers scan checks and any associated payment coupons through a check scanner attached to their PC and electronically transmit their deposits to the bank. Funds are automatically posted to their U.S. Bank account. Customers store deposited checks securely until they're destroyed. In the meantime, they gain prompt use of these funds without waiting for their next bank branch trip. Additional benefits include:

- Later depository deadlines. Customers aren't bound by their bank branch's business hours. Instead, they deposit checks at their convenience. Depository deadlines run as late as 10 p.m. Central Time for same-day ledger credit, depending upon location.

- Streamline banking relationships. On-Site Electronic Deposit operates regardless of geography or proximity to a U.S. Bank branch. Businesses can therefore eliminate local banking relationships and consolidate all of their activity with U.S. Bank.
- Prompt return-item notification. Expedited deposits yield faster notification of returned items. Acting on these transactions quickly improves customers' overall collection rates.
- More audit control. Customers can enhance internal security by allocating tasks to employees based on their function. One U.S. Bank customer segregates collection duties by having an employee in Arizona scan incoming checks while another person in Minnesota reviews and approves them for deposit. Another customer scans checks at its more than 500 locations, but one person in its central office approves them for deposit, eliminating the need to transport checks between offices.
- Enhanced data accuracy. Customers may capture remittance data during the scanning process and automatically post payment information to their accounts receivable systems. Automating these manual tasks saves time, improves efficiency and prevents human errors.

"If you have multiple business locations, On-Site Electronic Deposit lets you reduce costs by maintaining a single bank relationship and eliminate the time-consuming task of reconciling multiple accounts," Schmitt says. Contact your Treasury Management Consultant to learn how your business can benefit from streamlined cash and check deposits.

Minimize Fraud Losses Using Check Fraud Prevention Services

Spring 2011

The statistics are staggering—payment fraud activity is increasing at a rapid rate. According to the 2010 AFP Payments Fraud and Control Survey, 73% of organizations experienced attempted or actual payment fraud in 2009, and 30% reported that incidents of fraud increased from 2008 to 2009. Furthermore, 90% of organizations that experienced attempted payment fraud were the victims of check fraud.

“Although electronic payments are increasing in popularity, check fraud continues to be where companies are most vulnerable,” says Michele Johnson, U.S. Bank Vice President, Global Treasury Management, Commercial Product Management. “It’s not a matter of if your organization will be the victim of an attempted payment fraud. It’s a matter of when.”

Checks remain the payment method most frequently targeted by fraudsters. Their methods range from counterfeiting checks to altering payee names and dollar amounts. “We want to partner with customers to create customized fraud prevention services in an effort to prevent the loss,” Johnson says. “Because once the loss occurs, it’s too late.”

In a recent groundbreaking court case, a bank won a lawsuit against a customer’s insurance company because the customer failed to implement Payee Positive Pay after being offered it by the bank. The customer later suffered a \$150,000 altered payee check fraud loss. “In light of this ruling, it’s likely that banks will include provisions in their contracts that limit their liability when their customers don’t implement fraud prevention services such as Positive Pay,” Johnson says. “As a result, it’s that much more crucial for organizations to reassess the services they currently have in place.”



U.S. Bank offers a broad range of check fraud prevention services to protect you from losses, including:

Positive Pay

Positive Pay solutions provide protection for a variety of accounts, payment types and business situations. “For accounts that are used to issue checks, Positive Pay is really the best fraud prevention tool offered by banks,” Johnson says. “Positive Pay is easy to use and it’s totally automated at U.S. Bank, which makes it highly effective at preventing check fraud.”

With Positive Pay, fraud is detected by matching checks presented for payment with your list of issued payments. Using U.S. Bank SinglePoint® Positive Pay, our integrated suite of Web-based services, you review the exceptions, view check images, make payment decisions, request adjustments and access history online.

Spring 2011

There are a variety of additional fraud prevention services available that can be tailored to meet unique needs, including:

- **Check Filters** – Block all checks from posting or just those over a given dollar amount. For example, specify a maximum check amount that is allowed to post to an account. “Applying a check filter is an ideal service for deposit-only accounts or specialty disbursement accounts where you do not issue checks over a certain amount,” according to Johnson.
- **Reverse Positive Pay** – The bank sends you a daily file of paid items showing dollar amount and serial number. SinglePoint gives you the ability to view the item images and determine any items that should be returned.
- **Positive Pay** - Account number, serial number and dollar amount are checked at the teller and in the back office. Customers review exception items on SinglePoint and direct the bank to either pay or return them.
- **Teller Payee Positive Pay** - Payee information is verified at the teller.
- **Payee Positive Pay** - Payee information is verified in the back office and at the teller line.
- **Teller Positive Pay Special Handling** - Payee information provided by the customer is verified through a customer service line.

U.S. Bank offers a broad range of service options to meet your specific needs. “Given the increase in check fraud and the recent court ruling, we’re urging our customers to step back, understand the various service options available, assess what they need, select appropriate options, and then fully utilize each service to make it as efficient as possible in preventing check fraud loss,” Johnson says.

Contact your Treasury Management Consultant to learn how your business can benefit from these strategies.

Positive Pay Prevents \$1 Million Loss

Recently, a large number of checks suddenly appeared as exceptions on one of our customer’s Positive Pay accounts. By viewing the check images, the customer discovered its account was being used in a bogus lottery scheme. Thankfully, the timely return of the exception items prevented losses of \$1 million.

The Power of Green

Spring 2011

Golf and the Environment

earthshare.org

Next time you are out on the greens, think about whether your own actions are "green." Here are some easy suggestions on what you can do to help the environment:

- **Walk** the course instead of using a golf cart. If you do use a golf cart, keep your cart on the designated path.
- **Replace** all divots.
- **Urge your golf course to replace** its carts with electric-powered ones, which greatly reduce both air pollution and noise pollution.
- **Carry your trash** with you until a waste container is available.
- **Recycle** glass, aluminum, and plastic on the golf course. If your course doesn't have its own recycling program, urge them to start one.
- **Adhere to local rules** that may restrict access to environmentally sensitive areas on a golf course.
- **Buy recyclable products** (biodegradable golf tees, golf balls made of rawhide instead of plastic).
- **Accept the natural limitations** and variations of turf grass plants growing in a natural environment (e.g., brown patches, thinning, loss of color). Be willing to play on brown grass during periods of low rainfall.
- **Patronize** courses that are environmentally friendly.
- **Recognize** that golf courses are managed land areas that should complement the natural environment. Respect environmentally sensitive areas of the course.
- **Support** golf course management decisions that protect or enhance the environment and encourage the development of environmental conservation plans.
- **Support maintenance** practices that protect wildlife and natural habitat.



- **Encourage maintenance** practices that promote the long-range health of the turf and support environmental objectives. Such practices include aerification, reduced fertilization, limited play on sensitive turf areas, reduced watering, etc.
- **Commit to long-range conservation efforts** (e.g. efficient water use, integrated pest management, etc.) on the golf course and at home.
- **Support research and education programs** that expand our understanding of the relationship between golf and the environment.