Remote Deposit, one of the more exciting cash management products introduced in recent years, allows businesses to use desktop scanners to capture images of paper checks and securely transmit them to the bank over the Internet for deposit. This expedited receivables process saves businesses the time and money associated with daily bank trips or employing armored car services.

To reduce any associated risks and protect their customers’ check data, it’s recommended that Remote Deposit users follow a number of best practices.

**Protect customer information**
One of the most important of these best practices is to secure customer checks after scanning. You want to protect information such as check MICR line data (e.g., account and routing and transit numbers and payor’s signature) from being stolen and used to commit payment fraud.

Once checks are scanned, they should be stored securely and maintained under dual control until they are destroyed. “Destruction, preferably through shredding, will help protect your customer information and eliminate the risk of duplicating a deposit,” advises Ricky Stevens, a Capital One Bank product manager.

**Remote Deposit best practices at a glance**
- Calculate your deposit total prior to scanning checks and make sure your scanned deposit total matches your calculated deposit total.
- Store scanned checks with printed deposit documents immediately after scanning.
- Use dual control practices to restrict access to your deposited checks.
- Destroy scanned checks by shredding.

**Daily Remote Deposit cutoff extended**
Capital One Bank extended its daily Remote Deposit deadline to 8 p.m. Eastern Time/7 p.m. Central Time. This extension gives you additional time to deposit checks through Remote Deposit for same-day credit.

**Eliminate redeposit risk**
Physically securing scanned checks under dual control and destroying them in a timely manner reduces the risk that these items could be redeposited, Stevens says.

Capital One Bank’s Remote Deposit system prohibits deposited items from being redeposited electronically for 90 days.

**Ensure deposit accuracy**
There are also a number of best practices for helping to ensure Remote Deposit accuracy. For example, it is recommended that you always calculate your deposit total prior to scanning checks, and make sure that your scanned deposit total matches your calculated deposit total.

Another key recommendation is to endorse your checks prior to depositing them, if your scanner does not automatically do so.

**Best practices recommendations**
Capital One Bank has developed a comprehensive list of best practices recommendations that addresses risk related issues for Remote Deposit users. To acquire a copy, please contact your Treasury Management advisor.
Make cross-currency payments online

It’s more efficient and appreciated by trading partners

Capital One Bank® business clients can initiate foreign currency wires online — and soon they will be able to do so in more currencies than ever before. Enhanced cross-currency payment capabilities through the bank’s Treasury Optimizer® Internet-based banking portal will be available this fall.

Treasury Optimizer’s cross-currency payment functionality adds speed, accuracy and efficiency to transactions, according to Henry Gorbet, senior vice president and head of Electronic Services, Treasury Management, at Capital One Bank. Plus, it can be a boon to supplier relations, he says.

“Clients just go online, view the current exchange rates for the foreign currency to which they are converting U.S. dollars, and initiate the transaction,” he explains. “It’s much more efficient than a manual process, where you must call a banker, who in turn must talk to someone in the bank’s Foreign Exchange area to determine the exchange rate.”

For the many companies that today are sourcing goods and raw materials from foreign trading partners, paying in the supplier’s currency is a relationship booster. Most suppliers will appreciate no longer being subject to foreign exchange related fees from intermediary banks, which can reduce the size of the payments they ultimately receive.

Capital One Bank is expanding the number of currencies in which users can send cross-currency wires. Through Treasury Optimizer, clients will be able to initiate cross-currency payments in 25 currencies. Plus, they will be able to make such payments in another 70 less-used currencies by contacting a Capital One foreign exchange trader.

Checks still biggest fraud threat

If you want to reduce payments fraud risk, issue fewer checks. That’s the core message for treasury managers from the Association for Financial Professionals (AFP) 2010 Payments Fraud and Control Survey*.

The survey results indicate that check fraud remains the major source of payments fraud. Some 73% of organizations experienced attempted or actual fraud in 2009, and within that group 9 out of 10 were victims of check fraud. Meanwhile, other payment types targeted for fraud lagged well behind. Automated Clearing House (ACH) debits were the second most targeted (25%), followed by consumer credit/debit cards (20%), corporate/commercial cards (17%), ACH credits (7%) and wire transfers (3%).

The leading check fraud technique reported by respondents was counterfeit checks using an organization’s MICR line data (72% of respondents), followed by altered payee names (58%) and altered dollar amounts (35%).

When check fraud resulted in losses to an organization, 37% said it involved a check being cashed by a check-cashing service. Another common loss factor, cited by 20% of respondents, was “account reconciliation or positive pay review not being timely.”

Move to ACH, card payments

Many of the survey respondents that had shifted from paper to electronic payments indicated they had done so with fraud prevention in mind, a strategy that AFP applauds. “Organizations large and small should be pushing hard and working with their banks, vendors and other suppliers to eliminate this [check fraud] vulnerability by moving transactions to ACH and card payments,” the AFP survey report advises.

To learn how Capital One Bank can help you manage payments fraud, please contact your Treasury Management advisor.

* The source of all survey results cited in this article is the AFP’s survey report at http://www.afponline.org/pub/pdf/2010_Payments_Fraud_Survey.pdf.
Follow payment card security rules to avoid costs, reputation damage

Merchants that accept credit or debit cards must comply with standards established in recent years by the major card associations to safeguard buyers' card data. Failure to meet these standards can result in costly fixes, hefty fines and crippling reputation damage.

Technology enabling merchants to accept card transactions over the Internet — and some card-data breaches that followed — led the card associations to collaborate on the Payment Card Industry Data Security Standard (PCI DSS). The standard attempts to prevent unauthorized access to cardholder data, such as a skilled hacker remotely accessing a computer system containing cardholder records.

The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other measures intended to protect customer card data.

Reasons to comply
The card associations — MasterCard Worldwide, Visa Inc. International, Discover Financial Services, American Express and JCB International — are responsible for enforcing compliance with the standard. They in turn rely on acquirers, like Capital One Merchant Services (COMS), to ensure their clients comply. Potential consequences if a merchant doesn’t adhere to PCI DSS and has its system hacked into and customer card data stolen include:

- **Expensive remediation.** If the card associations notify COMS that your business is the source of a card-data breach, you will need to shut off your Internet connection and submit to a costly forensics investigation to determine the reason for the breach and steps to fix the problem.

“Qualified Security Assessors [QSAs] typically charge $10,000 to $20,000 per business location to conduct an investigation,” says Chris Hartner, PCI compliance manager at COMS.

- **Potentially large fines.** When the investigation is complete, the QSA firm will send a report on its findings to the card associations. “Based on that report, including how egregious the security lapses were and how many cards were compromised, the card associations will levy a fine,” Hartner says. “The fines I’ve seen have ranged from $5,000 to $200,000.”

- **Damage to your business’s reputation.** A compromised merchant faces the threat of negative publicity and resulting damage to the reputation it has worked so hard to build. “Many businesses that experience card-data security breaches end up on the evening news and in the newspapers,” Hartner says.

Mandatory compliance program
COMS requires clients that process card transactions over an Internet connection to participate in a PCI DSS compliance validation program through security vendor ControlScan. Merchants take a self-assessment questionnaire that reviews the policies and procedures they employ to store, process and transmit credit card data, and train their staffs. They must annually complete and pass the questionnaire, and each quarter must pass a network scan of their system, in order to remain compliant with PCI security standards.

If you have questions about the standards or how to remain in compliance, visit www.controlsan.com/capitalone or call ControlScan at (800) 642-2542.
Inside Treasury Management

No company is immune to disaster. Whether it’s due to wildfires or earthquakes in the West, tornadoes or flooding in the Midwest, hurricanes in coastal areas, or terrorism just about anywhere in the country — every organization faces the risk that someday a disaster will hit and threaten to interrupt their business and play havoc with their cash flow.

That’s why corporate treasury departments need to invest in the development of a well-conceived disaster recovery plan, one that leverages bank products and other technology to support recovery efforts.

“A good disaster recovery plan is like an insurance policy. You have to spend money to set it up and maintain it, and the plan doesn’t generate any revenue,” says Ken Smiley, senior vice president and Treasury Management sales manager for Louisiana, Texas and the Mid-Atlantic at Capital One Bank. “But if a disaster occurs, you will be glad you have a recovery plan.”

**Disaster planning basics**
Planning for a disaster can be the key to your business’ survival, and there’s much to include in your recovery plan. Begin by identifying the risks — the kind of disasters you’re most likely to experience — and then develop a detailed plan for how you will respond to each type of disaster.

You need to prioritize critical treasury functions (e.g., vendor and payroll payments, the ability to initiate payments to employees and contractors to cover daily expenses such as supplies, and lockbox collections) and how quickly these must be recovered. It’s also important to establish a means for treasury employees to work off-site and access critical back-up systems, records and supplies.

At least once a year you should update and test your plan, as well as meet with stakeholders such as banks, trading partners and vendors to discuss critical components of the plan that require their participation.

**Cash management contingency planning**
Here are some contingency planning guidelines that specifically relate to the treasury department’s challenge of continually meeting the company’s cash flow needs:

- Fund bank accounts and keep enough cash on hand to handle immediate needs.
- Take your credit cards in the event of an evacuation.
- Use Internet banking services to monitor account activity, manage cash flow, initiate wires and pay bills.
- Reduce dependency on paper checks and postal service to send and receive payments (consider using direct-deposit/direct-debit electronic payments and remote deposit banking services).
- Contact your branch for any special coin/currency needs, if a threat is imminent.
- Make night depository drops as early as possible, if a threat is imminent.
- Prepare to safeguard your own deposits in the event you are unable to reach a branch that can process your transactions (consider using remote deposit banking services).

**Help in developing a plan**
Look to Capital One Bank for assistance with your contingency planning efforts. Talk to your Treasury Management advisor, and be sure to visit our Web site to access a detailed business disaster planning checklist (www.capitalonebank.com/disasterplanning).

In addition to some of the planning tips noted in this article, the checklist includes guidelines for establishing alternative operational locations and backup sites, safeguarding company property, maintaining communications with employees and customers and ensuring they are ready for a disaster — as well as post-disaster recovery procedures.

There is no substitute for the advice of experts with intimate knowledge of your operations. We at Capital One, National Association recommend that you obtain data security and anti-fraud advice from such experts. While we may provide you with some recommendations regarding controls or best practices from time to time, these recommendations cannot replace the services of dedicated data security and anti-fraud experts with a true understanding of your business.
Direct deposit offers opportunity to reduce costs, ‘go green’

Fewer than three-quarters of U.S. employees (72%) receive their pay electronically, according to results of the PayItGreen Survey 2010*, suggesting that many companies are missing an opportunity to reduce costs, provide an appreciated employee benefit and protect the environment.

The primary reason cited by respondents for still receiving a paper paycheck is that their employers don’t offer direct deposit of payroll, according to the survey conducted by PayItGreen, an industry coalition led by NACHA – The Electronic Payments Association that is dedicated to promoting the positive environmental impact of electronic payments. “The level of participation in direct deposit of payroll in the United States pales in comparison to some other developed countries where nearly all employees receive their pay electronically,” notes Linda Adams, Treasury Management product director at Capital One Bank®.

The PayItGreen survey results indicate that some of the biggest lost opportunities are at companies with fewer than 100 employees. Less than half of their employees (48%) say they are participating in direct deposit of payroll.

Why direct deposit?
It appears many companies aren’t taking advantage of major potential savings. According to the survey, companies can save from $2.87 to $3.15 per payroll payment by using direct deposit. In fact, direct deposit can save a business with fewer than 100 employees $19,000 a year, PayItGreen reports.

Direct deposit also saves time and enhances productivity. Employees who aren’t on direct deposit spend between 8.5 and 24 hours a year making trips to cash or deposit their paychecks, the survey reveals. PayItGreen estimates that in the United States this results in $3 billion to $5 billion in lost productivity.

‘Going green’ benefit
Direct deposit offers an environmentally friendly approach to payroll, which employees appreciate, the survey says.

Electronic paychecks can drastically reduce an employer’s carbon footprint. According to PayItGreen, if a business that employs 300 people and issues paychecks every two weeks switches to direct deposit of payroll, in one year it would:

• Save 121 pounds of paper
• Avoid releasing 1,159 gallons of wastewater into the environment
• Save 45 gallons of gas
• Avoid releasing 346 pounds of greenhouse gases into the atmosphere

Of those survey respondents enrolled in direct deposit, 55% said they find such “green” benefits very or extremely motivating in terms of encouraging them to have their pay deposited electronically.

Calculate the benefits yourself
There are a couple information-packed Web sites that, among other things, can help a treasury manager calculate the benefits of switching employees to direct deposit of payroll.

One is www.electronicpayments.org, a NACHA-sponsored site that offers a “cost calculator” for estimating the savings an organization can achieve by moving to direct deposit. The other is www.payitgreen.org, which includes a “direct deposit calculator” that allows you to estimate how much you will be able to reduce the environmental impact of your business by switching employees to direct deposit from paper paychecks.

Additionally, look to your Capital One Bank Treasury Management advisor for guidance on how your organization can benefit from not only direct deposit of payroll, but also other forms of electronic payment. “Capital One Bank offers a full suite of Automated Clearing House products to meet the needs of any size business, including direct deposit of payroll, vendor payments, tax payments, and both business-to-business and business-to-consumer collections,” Adams says.

* The source of all statistics in this article attributed to PayItGreen or the PayItGreen Survey 2010 is a June 22, 2010, NACHA – the Electronic Payments Association news release. The release is online at http://www.nacha.org/news/newsDetail.cfm?RecentBusinessNewsID/161.
Capital One Bank’s Mid-Atlantic expansion cements its role as one of the nation’s top 10 banks (based on deposits) and ushers in an array of enhanced treasury management product offerings for clients across all of its markets.

The integration of Chevy Chase Bank, acquired by Capital One Financial Corporation in early 2009, took a major step forward with the September 13 name change. Capital One Bank® now has nearly 1,000 branches and more than 2,000 ATMs primarily in New York, New Jersey, Louisiana and Texas — the bank’s previous footprint — and now in Maryland, Virginia and Washington, DC.

“We’re excited to welcome our new Mid-Atlantic market clients to banking with Capital One Bank,” says Chris Ward, head of product management, innovation and integration, Treasury Management. As a result of the integration, customers will benefit from numerous treasury management service options and enhancements, including an expanded lockbox network, lockbox imaging, a Virtual Vault service, extensive card solutions and the Capital One Deposit Center™, which supports remote deposit of checks and card acceptance using a single piece of hardware. “Capital One Bank is ready to serve you, and we’ll continue to provide the superior level of service you’ve come to expect from the same proven team,” Ward says. “You can also be confident in Capital One Bank’s strength and stability.”

The integration has driven a host of product developments that will benefit all Capital One Bank clients. “We’ve upgraded our ACH and file transfer platform; extended deadlines for Positive Pay exceptions, ACH transactions and wire transfer initiation; and improved cash concentration and controlled disbursement offerings,” Ward says. “We’re also moving to a consistent information reporting platform across our franchise.”

If you have questions about the recently completed integration of Chevy Chase Bank and Capital One Bank, call your Treasury Management advisor.