

As we continue our journey into the Internet age, many of the transactions we used to perform face to face have become electronic. Banking is no exception. Transactions that seemed time consuming and required enormous amounts of written documentation have gone paperless, or “green.” The implications are endless, as are the challenges to secure the data and the assets this data represents. This whitepaper will review some of the opportunities offered through electronic banking and some guidelines for making the most of this technology.

What is Electronic Banking?

To most people, electronic banking means 24-hour access to cash through an automated teller machine (ATM) or paychecks deposited directly into checking or savings accounts. Technically speaking, electronic banking makes use of a process known as electronic funds transfer (EFT).

Electronic funds transfer refers to the movement of funds from one bank account to another by means of electronically communicated payment instructions. EFT allows companies to pay or collect corporate obligations, and exchange payables and receivables information electronically. Settlement of funds takes place among all parties on an agreed upon date.

EFT has become a significant factor in day-to-day commercial transactions. Electronic payment and receipt of funds offers significant advantages over conventional processing techniques. Businesses have increasingly implemented EFTs as a means to reduce costs and paperwork (improving operating efficiency) and to better control their receivables and payables.

To initiate an EFT, a company must enter into an agreement with a financial institution capable of originating these transactions. The company needs to obtain written authorization from its customers and suppliers allowing for deposits or charges to their accounts. All parties can then agree on responsibilities and the manner in which entries will be processed and settled.

When making electronic funds transfers, the suppliers receive credit to their corporate account along with invoice information. When an EFT is used to collect payment due, the customer's corporate account is debited and information to update their payables is provided.

Functionally, EFT includes two principal categories: credit transfers and debit transfers. A credit transfer is one in which the originator instructs its bank (via a payment order) to transfer funds belonging to the originator for credit to the beneficiary's account (i.e., the instruction to pay is given by the person making the payment). A debit transfer is one in which the originator instructs its bank (via a payment order) to collect funds on behalf of the originator by debiting another party's account at the other party's bank (i.e., the instruction is given by the person receiving payment).

What are Examples of EFT in Operation?

The EFT mechanism moves money between accounts in a fast, paperless way. Below are some examples of EFT systems in operation:

- **Automated Teller Machines (ATMs)** PTAs could do their banking without the assistance of a teller. A PTA could obtain cash, make deposits, pay bills, or transfer funds from one account to another electronically. These machines are accessed using a debit or credit card and a code, which is often called a personal identification number or "PIN." A receipt may be issued at the close of the transaction or obtained online at a later date to itemize the transaction details.
- **Point-of-Sale (POS)** Some debit or check cards can be used when shopping to allow the transfer of funds from the PTA's account to the merchant's. To pay for a purchase, the PTA presents a debit or credit card instead of a check or cash. Money is taken out of the PTA's account and put into the merchant's account electronically. Again a receipt is

issued at the close of the transaction to itemize the details of the transaction.

- **Preauthorized Transfers** This is a method of automatically depositing to or withdrawing funds from a PTA's account when the account holder authorizes the bank or a third party (such as an employer) to do so. For example, PTA could authorize direct electronic deposit of wages, Social Security, or dividend payments to their accounts. Or they could authorize financial institutions to make regular, ongoing payments of insurance, mortgage, utility, or other bills. A receipt is issued via e-mail or postal mail confirming or reminding payment was applied and itemizing the transaction details.
- **Telephone Transfers** PTAs could transfer funds from one account to another—from savings to checking, for example—or can order payment of specific bills by phone. By providing the operator with the debit or credit card information or the checking account details, a transaction may be completed by telephone. A receipt is mailed, faxed, or e-mailed itemizing the details of the transaction.
- **Computer Banking Services** offers the convenience of conducting many banking transactions electronically using a personal computer or other electronic devices. Individuals can view account balance, request transfers between accounts, and pay bills electronically from offices or home.

Types of Electronic Currency

1. **Check cards**, the new name for debit cards, can be used instead of cash, personal checks, or credit cards. When a PTA use a check card, you transfer funds immediately from The PTA account to the store's account. A growing number of consumers use check cards

because they eliminate the hassle and risks of writing checks or carrying large amounts of cash. Important facts PTAs need to know are:

- a. You have less bargaining power with a check card than with a credit card. With a credit card you have the right to refuse to pay for the purchase if you are not satisfied. With a debit card you have already paid for the product, so you have less bargaining power with the merchant.
- b. A thief with your check card and PIN number can take all the money in your account. The thief can even make point-of-sale purchases without your PIN.

Note: Some check card providers have voluntarily capped the loss liability of check card holders at \$50. "As welcome as these voluntary protections are, they are too important to be left to the kindness of bank marketing departments," writes Consumer Reports. The consumer advocacy magazine advocates federal law changes to make consumer liability caps mandatory.

In an era of increasing bank fees, PTAs can expect to pay for the service of using a check card.

It is the PTA's responsibility to keep check card receipts and record the dollar amounts of the purchase deducted from the PTA bank balance immediately, in order to avoid overdraft changes.

2. **Smart cards**, sometimes called stored-value cards, have a specific amount of credit embedded electronically in the card. For example, a \$100 smart card that you have purchased in advance can be used to cover expenses such as pay phone charges, bridge or expressway tolls, parking fees, or Internet purchases. These cards make the transaction fast, easy, and convenient. Smart card technology is in a period of rapid change. Ultimately PTAs should be able to customize their smart cards to suit their financial

needs with access from their personal computer or mobile phone. Some important consumer issues are:

- a. Smart cards are the equivalent of cash, so they must be guarded.
- b. Procedures for recovering the value of a malfunctioning smart card are unclear.
- c. The computer chip within the card will contain both financial and personal information. Privacy and security issues could be a problem.

Smart cards may not be covered by the in case of loss or misuse of the card.

3. **Digital cash** is designed to allow the PTA to pay cash rather than use a credit card to purchase products on the Internet. One type of digital cash allows PTAs to transfer money from a financial institution or a credit card into an "electronic purse." The cash is held in a special bank account that is linked to your computer. Another type of digital cash converts money into digital coins that can be placed on your computer's hard drive.
4. **Digital checks** allow PTAs to use their personal computers to pay recurring bills. PTAs could use computer software provided by a bank, or they could use personal finance software packages such as Quicken or Microsoft Money and subscribe to an electronic bill-paying service.

The technology of paying bills electronically by home computers is advancing rapidly, but relatively few businesses currently can accept payments made directly by computers. Digital checking is expensive. Fees generally run from \$5 to \$10 a month for 20 transactions. Privacy and security issues are major consumer concerns. Encryption technology may lessen privacy concerns in the future.

Why Consider EFT (Electronic Funds Transfer)?

Businesses have feared that an electronic solution would be too complicated and costly to implement and don't want to change their current methods of deposit. However, companies that have embraced EFT are enjoying immediate benefits from increased cash availability, reduced risk of fraud, and lower costs for check processing.

The cost of moving checks through the banking system is estimated to be about \$3.50 or more per check, including the costs of paper, printing, and mailing. Moreover, checks (except your own check presented at your own bank) take time to cash: time for delivery, endorsement, presentation to another person's bank, and time to wind through various stations in the check-clearing system. Technology now can lower the costs of the payment mechanism (to about \$1.50 or less per transaction) and make it more efficient and convenient by reducing paperwork.

Additionally there are 18 Reserve Banks, all currently handling and processing paper checks. By 2010 only four of these banks are scheduled to continue processing paper checks. This will increase the overall cost of using paper to transact business.

How are Transactions Recorded?

A cancelled check is permanent proof that a payment has been made. But what proof of payment is available with EFT services?

If a PTA used an ATM to withdraw money or make deposits, or a point-of-sale (POS) terminal to pay for a purchase, you can get a written receipt—much like the sales receipt you get with a cash purchase—showing the amount of the transfer, the date it was made, and other information. This receipt is your record of transfers initiated at an electronic terminal.

A PTA's periodic bank statement must also show all electronic transfers to and from your account, including those made with debit cards, by a preauthorized arrangement, or under a

telephone transfer plan. It will also name the party to whom payment has been made and show any fees for EFT services (or the total amount charged for account maintenance) and your opening and closing balances. Your monthly statement is proof of payment to another person, your record for tax or other purposes, and your way of checking and reconciling EFT transactions with your bank balance.

How Easily Will Errors be Corrected?

The way to report errors is somewhat different with EFT services than it is with credit cards. But, as with credit cards, financial institutions must investigate and correct promptly any EFT errors you report.

If you believe there has been an error in an electronic fund transfer relating to the PTA account:

- Write or call the financial institution immediately if possible, but no later than 60 days from the date the first statement received shows an error was mailed. Give the PTA's name and account number and explain why you believe there is an error, what kind of error, and the dollar amount and date in question. If you call, you may be asked to send this information in writing within 10 business days.
- The financial institution must promptly investigate an error and resolve it within 45 days. However, if the financial institution takes longer than 10 business days to complete its investigation, generally it must put back into your account the amount in question while it finishes the investigation. (The time periods listed above are longer for POS debit card transactions and for any EFT transaction initiated outside the United States.) In the meantime, you will have full use of the funds in question.
- The financial institution must notify you of the results of its investigation. If there was an error, the institution must correct it promptly—for example, by making a re-credit final.

If it finds no error, the financial institution must explain in writing why it believes no error occurred and let you know that it has deducted any amount re-credited during the investigation. You may ask for copies of documents relied on in the investigation.

What about Loss or Theft?

It's important to be aware of the potential risk in using debit card, which differs from the risk on a credit card.

- On lost or stolen credit cards, your loss is limited to \$50 per card. On a debit card, your liability for an unauthorized withdrawal can vary.

What Insurance Coverage is Available?

Crime coverage (package 3) policy provides for a multitude of crimes, including online and electronic banking. This coverage is relatively inexpensive for the additional security provided. Your insurance broker or agent can provide details and a checklist for coverage available under this package. Even with proper insurance coverage, any PTA utilizing EFT processes should always have the latest computer virus protection available.

What Should a PTA Consider Before Moving to Electronic Banking?

For PTAs, electronic banking simply replaces one method of banking (brick and mortar and pieces of paper) for another (websites, passwords, and confirmations). The real challenge remains the same. How do we approve, record, and track each transaction accurately?

The *Money Matters Quick-Reference Guide* covers ways to secure, record, and handle cash. PTA's Theft, Fraud and Embezzlement white paper discusses the importance for internal controls. Those recommendations can be updated to apply here within the electronic banking arena.

Electronic banking for this discussion can be broken into three parts: payments, deposits, and bank reporting activities. The technology used by banks can differ in both cost and features offered.

Electronic banking can be secured through user names and passwords. The security established can be done by roles or functions described within one's job description. It is very important for security that no one person wears too many hats, and that the number of authorized users for credit and debit cards (or other EFT methods) be kept as small as possible.

General Electronic Banking Controls

Approving Transactions

Current Process:

Money Matters recommends PTAs require in their bylaws that all payments have two signatures on each check. When making payments online no signatures are required. How can PTAs maintain the two signature recommendation?

Many PTA bylaws require dual signatures on all checks. If this is the case with your PTAs bylaws, they may need updating to include electronic payment processing or electronic banking processes. You may want to look into this sooner rather than later, as by 2010 only 4 of the 18 Federal Reserve banks will continue to process paper checks.

Recommendation:

Most online banking processes allow for one person to make the initial request. Generally an e-mail is forwarded to a second person to confirm the request and complete the process. An e-mail is sent with transaction details, including amounts, dates, and transaction numbers for the PTA's permanent records. This e-mail address can be to the accounting department responsible for tracking and recording the transactions on the PTA's books. This dual approval process can replace or augment the more traditional two signature approval.

Example:

Electricity bills can be made online. The standard process follows:

An e-mail is sent from the utility company to the person responsible for tracking utility payments, such as the purchasing agent.

The purchasing agent will use the link in the e-mail from the utility company to visit the utility's website. After logging in, the purchasing agent can download, review, and submit the bill for approval to the treasurer. Approval can be obtained from the treasurer by attaching an electronic copy of the bill to an e-mail stating "I approve payment for the attached bill in the amount of \$\$\$\$\$. Please charge account number #####-#####-####."

The accounts payable person or the person acting as the second signature would then go online and pay the bill. A confirmation will appear on screen. This can be printed and saved electronically. In an electronic file folder, like those created to save Word documents or vacation photos, an electronic copy of this payment and the bill would be saved. This folder can be organized by month, by vendor, by event, or by some other standard filing method.

A similar method of approval and payment may be established for any process the PTA wishes to complete electronically.

The most important key will be the consistent and complete documentation of each invoice and corresponding payment. The PTA can maintain both paper and electronic copies until a process is developed to ensure that all payments have the supporting documentation and the information can be located as required for auditing and periodic reconciliation purposes.

Securing Passwords:

What steps should a PTA take to secure passwords used for electronic banking?

As with any type of login-password security, the following are just some basic points to keep in mind:

Do not share logins or passwords.

Each individual providing a function to or serving a role in using electronic processing **MUST** have their own unique login and password. Sharing this information defeats all security and rationale for establishing security.

Passwords should have an expiration date.

In order to keep your processes secure, password expirations are necessary. It is generally recommended that passwords expire during a 60-90 day range.

Once passwords are provided to the user, no written record should exist.

Once logins and passwords are issued, they become the responsibility of the user to remember. If the user loses their password, the old password is removed and a one-use temporary password should be provided for the user to then update and maintain.

Access to any system should be reasonable and based on need.

Some PTAs should limit system access to only hired staff; others PTAs may extend access to the elected officers. Regardless of who has access, reasonable control must be maintained. Many

electronic banking processes allow for read- or view-only access in addition to limited processing (like creating or requesting payments or payment only processes). These controls can limit unnecessary access to PTA assets.

Other Good Accounting Precautions:

What other things should PTAs be in the habit of doing in regards to incorporating EFT into unit procedure? Security expert Kevin Coffey recommends the following:

- Sign your new debit and credit cards as soon as they arrive.
- Carry your PTA debit and credit cards separate from your wallet.
- Keep a record of your card numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep your card in view, whenever you can, after you give it to a clerk. Retrieve your card promptly after using it.
- Don't sign blank receipts and draw a line through blank spaces above the total when you sign card receipts.
- Void or destroy incorrect receipts.
- Open billing statements promptly and reconcile your card accounts each month.
- Notify card companies in advance of a change in address.
- Never lend your card(s) to anyone.
- Never leave your cards or receipts lying around.
- Never put your card number on a postcard or on the outside of an envelope.
- Never give your number over the phone unless you are initiating a transaction with a company you know is reputable. If you have questions about a company, check with your local consumer protection office or Better Business Bureau before ordering.

Services:

What products are available for PTAs with regard to electronic banking?

There are an infinite number of products related to electronic banking and any related component within this process.

The first place to start should be your current financial institution. They offer a number of products and services that are Internet-ready and have established security protocols in place. In some cases this may be the simplest and most beneficial option.

PTAs with software products currently in place can request information from their software provider to guide them in identifying what service and information can be automated to streamline their current business processes. Most software packages can link to your banking system for processing much like your personal banking products.

There are third party products available, such as PayPal and Xoom, that allow additional levels of security for smaller PTAs. These products allow for dual processing of payments and deposits through the Internet. For example, orders can be placed and PayPal used as the payee. The invoice is sent to the PayPal account for payment. After logging into the PayPal account, the invoice can then be approved for payment. The person confirming the payment through PayPal can approve payment using digital cash, a credit card, or other EFT options.

All of the above products and services provide electronic receipts, e-mail confirmations, and detail tracking (including options to reconcile transactions to monthly banking statements).

To EFT or Not EFT: Weighing a PTA's Options

How will a PTA know what option is right for them? PTAs will need to look honestly to the strengths and weaknesses of their current business processes.

If the PTA's current environment has weak business processes resulting in poor internal controls, this must be addressed prior to or in conjunction with transitioning to an electronic environment. Taking weak and ineffective business processes and moving them to an electronic environment will only make matters worse quickly. The need for complete and accurate documentation is more important in an electronic environment. The need to recognize, research, respond to, and correct a problem is time sensitive in the electronic realm.

Disclaimer:

The information, suggestions and recommendations found in this document 'Electronic Banking Whitepaper' are being provided for educational and informational purposes only. They are not intended to, and do not constitute, legal advice. Local units should check with their local attorneys or state regulators for relevant laws and regulations.

Resources:

- E-Banking- banking on the Internet. Federal Reserve Bank of New York
- Electronic Banking Basics. Federal Trade Commission (FTC) online at www.federalreserve.gov
- Wells Fargo: Electronic Check Processing Business case kit Treasury management White paper
- Electronic Banking <http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre14.shtm>
- Electronic Banking (August 2003) US Dept of Treasury: Published Pamphlets <http://www.occ.treas.gov/netbank/netbank.htm>
- How to Guard Against Credit and Charge Card Fraud www.kevincoffey.com