

| | |
|---------------------|--|
| NEWSLETTER | <h1>PFC Journal</h1> |
| | |
| | |
| | |
| | |
| October 2003 | <h2>Philadelphia Financial Center</h2> |
| | |

**President of the United States Visits Philadelphia Regional Financial Center
Kicks Off First of Three Child Tax Credit Payment Cycles**



On July 24, 2003, President George W. Bush visited the Philadelphia Regional Financial Center (PFC) to highlight the issuance of the child tax credit payments, which began July 25, 2003.

As more than 120 employees from PFC watched and listened, the President spoke about his economic plan, and the challenges and trials we have faced as a nation since September 11, 2001. He invited several American families to the event, met with them prior to the speech and used their stories to illustrate how this child tax credit will help boost the economy and provide relief to American families. More relevant to FMS and the Philadelphia Center, the President focused on our efforts to fulfill his promise to deliver these checks, bringing tax relief to the American people. Of the more than 23 million checks FMS

disbursed over the three-week period, the center in Philadelphia made approximately 5 million of those payments.

President Bush recognized the PFC employees for their dedication to the job, for working diligently to make certain that these payments get to the American people accurately and on time. “I know a lot of you are putting in weekend shifts. I know a lot of you are working really hard. And I am grateful, but more importantly, the American people should be grateful for the work you do right here,” said President Bush. Additionally, the President thanked the employees for the hospitality they extended to him and to the White House staff. He acknowledged our efforts by saying, “I want to thank those good workers who allowed me and the press corps to come and see you doing your job. It's not easy to do your job with a distraction—(laughter)—and I must confess that sometimes the Presidential entourage can be distracting. (Laughter.) But we want to thank you all for your hospitality, and most of all, thank you for being such great Americans and working so hard on behalf of the American people.”

| | |
|--|----------|
| INSIDE | |
| <i>President of the United States Visits PFC</i> | <i>1</i> |
| <i>Secure Payment System</i> | <i>2</i> |
| <i>Address Hygiene</i> | <i>2</i> |
| <i>Reclamations Made Easier and More Efficient</i> | <i>3</i> |
| <i>Proposed ACH Rule Change</i> | <i>4</i> |
| <i>NOC Provides Easy Fix to EFT Payments</i> | <i>4</i> |

Secure Payment System

The Financial Management Service (FMS) has developed the Secure Payment System (SPS), which is a secure windows-based internet browser application that enables users to prepare and submit payment schedules to FMS using the internet. SPS replaces the existing Electronic Certification System (ECS).

On June 30, 2003, FMS' Credit Accounting Branch in Hyattsville, MD successfully created payments utilizing SPS and the Philadelphia Financial Center (PFC) successfully processed the payments. The target date for PFC to begin implementation to its external Federal Program Agencies (FPAs) is scheduled for the first quarter of fiscal year 2004. We will be providing further guidance with implementation requirements, as we get closer to rolling out the system to our customer agencies.

SPS will retain the same functionality of creating and certifying schedules, but will provide additional features and will be more user-friendly. Unlike ECS, SPS can run from any user's personal computer that meets the minimum hardware and software requirements.

Each FPA will only be required to designate one Data Entry Operator (DEO) and one Certifying Officer (CO). However, FPAs are encouraged to designate more than one user to these positions to ensure adequate coverage for payment processing. The Security Administrator (SA) role in ECS will be eliminated in SPS. In addition, unlike ECS, SPS will not require a Master Certifying Officer (MCO) and Transmission Certifying Officer (TCO). All COs will have the same capabilities.

Every SPS user at your agency must have a smartcard, which will be used in conjunction with a Public Key Infrastructure (PKI) certificate for user authentication and document signing. FMS will provide all PKI certificates for your SPS users at no cost to your agency, but will only provide two (2) smartcards: one (1) for the DEO and one (1) for the CO, per FPA site. Your FPA will be responsible for procuring smartcards for additional SPS users.

PKI will eliminate the SecurID card currently used for ECS remote dialing into the FMS host and will also eliminate the ECS PC Security Module Board. Every computer used at your FPA to access SPS will require a card reader. FMS will provide one (1) card reader per FPA site. Your agency will be responsible for procuring additional card readers. Both the smartcards and card readers are available for purchase from the General Services Administration schedule.

In order for a user to obtain a PKI certificate, the user must appear in person at a PKI Registration Authority (RA) or Local Registration Authority (LRA). FPAs will be permitted to establish LRAs at their site and FMS will have a RA at our Hyattsville, MD location. LRAs will be at our Washington, DC location and the four (4) Regional Financial Centers (Austin, TX; Kansas City, MO; Philadelphia, PA; and San Francisco, CA). FPA personnel may appear at any of the FMS locations for certificate processing.

The PFC SPS training staff will create PKI certificates for all users while performing SPS training. Additionally, at that time, the FPA may establish users to the LRA position who will have the ability to create additional PKI certificates as required by the FPA. The locations of training sites will be announced at a future date.

Please visit the SPS website at www.fms.treas.gov/sps for additional information or you may contact Edward G. Zimmer at (215) 516-8026 or Bobbie J. Mickens at (215) 516-8074.

Address Hygiene

Will our mail be delivered on time? This is a question that every Federal agency asks at one time or another. Why? Because due to poor "Address Hygiene", many mail pieces are subject to additional and/or exception handling by the United States Postal Service (USPS) in order to be delivered to the proper address. The best way to assure that your mail is delivered accurately and timely is to ensure that your practice good "Address Hygiene".

What is "Address Hygiene"? "Address Hygiene" is the maintenance of accurate and up to date address data for recipients of your mail. In addition, it is the manner in which the data is provided in your payment file. This is very critical in the processing of payments together with delivery of your mail.

Agencies should periodically review their address files of payees to ensure that they are accurate and in accordance with Treasury Financial Manual, Part IV, Chapter 2055.50. An address can vary in the number of lines. Generally, there are anywhere between 3 and 6 lines in an address. The address should at a minimum consist of a payee name, street address, apt. # (if any), p.o. box,

city, state, and zip code. The data should be typed in all uppercase letters. Punctuation marks are to be omitted except for the use of commas to set off the names of more than two payees. Long addresses should be avoided unless necessary for postal identification. If you use a zip + 4 in your address, it must be separated by a hyphen. In addition, payment identification information should not appear adjacent to the zip code area.

Check issue data for foreign addressed payments should include a 3-digit foreign sorting code in the domestic ZIP Code location. If the payment file is submitted as a bulk file (electronic file transmission or on magnetic tape), the foreign sorting code should not contain leading zeros in the 5-digit zip code field; otherwise, it may be mistaken for a domestic zip code. A list of the foreign country sorting codes may be obtained from the Office of the Chief Disbursing Officer. Checks addressed outside of the United States must bear the name of the country, except for checks with APO/FPO addresses.

Some examples of bad "Address Hygiene"

- Incomplete street numbers and/or names
- Space between the lines of the address
- City and state on separate lines
- Missing and/or inaccurate zip codes and/or +4
- Phone numbers included in the address lines
- Address data typed in lower case letters

Did you make a change to your file format? This happens frequently due to changes in processes, regulations, policies and procedures. Programming changes in one area may sometimes cause unexpected changes in another area of the file. As good practice, when programming changes are made, agencies should review the entire address file to ensure that there have been no unwanted changes and that it supports proper address hygiene. An example of programming issues would be programmers using left justifications for the payee first and last name. This will create a large space between the names. Banks may balk at cashing checks of this nature.

Good "Address Hygiene" will benefit not only the payee, but the agency as well. This would prevent checks from being returned as non-deliverable by the Post Office. When checks are returned to the Philadelphia Financial Center, they are cancelled and the money is returned to the issuing agency. The agency will then reissue the payment with what it hopes is the correct address data. Good hygiene will reduce the number of checks returned, thereby reducing the amount of time and money spent to reissue payments.

Reclamations Made Easier and More Efficient

The Financial Management Service (FMS) is improving the current paper-based and time-consuming electronic funds transfer (EFT) reclamation process. Reclamations are notifications to a financial institution that the Federal Government requests the return of EFT benefit payments disbursed after the death of a Federal benefit payment recipient.

On the Internet, Pay.gov is a Government-wide transaction portal, managed by FMS, which offers a range of electronic financial services. FMS is starting to use Pay.gov to transmit automated EFT reclamation notices to financial institutions. Automated reclamations will be implemented in several phases.

Last spring, phase I of the Automated EFT Reclamation project was implemented as a pilot. This pilot included two volunteer financial institutions, Wachovia and World Savings, the Social Security Administration (SSA), and FMS' Philadelphia Financial Center. Phase I allows the financial institutions to receive their reclamation notices electronically through Pay.gov. Pay.gov creates the web-enabled forms and notifies the financial institutions by e-mail that there are reclamations that can be pulled down from the website. The financial institution, using a secured assigned PIN to access the site, views and downloads the form and processes under existing procedures. The operation is running smoothly, with the financial institutions processing the automated reclamations successfully.

Future phases include:

- Allowing the financial institution to complete the reclamation form online and return it to the Government
- Allowing the Government to accept electronic partial payments
- Enabling additional financial institutions to register to receive automated reclamations

For additional information or to address any questions, please contact Matt Helfrich at (215) 516-8020.

Proposed Rule to Expand Check Conversion & Provide Changes to Current ACH Rules

On August 21, 2003 the Financial Management Service (FMS) issued a proposed rule to amend 31 CFR Part 210, the rule governing the use of the Automated Clearing House (ACH) system by the Federal government. Each year, the National ACH Association (NACHA) issues rules on the ACH system that financial institutions and private sector companies must follow. However, the Federal government has a mission unique from the private sector, and FMS therefore issues a rule annually that accepts or modifies the NACHA rules. The public, financial institutions, private sector companies, and other Federal agencies have 90 days to comment on this proposed rule.

Last year, FMS issued rules that allowed Federal agencies to utilize a new technology called “check conversion”. Under check conversion, see <http://www.pcc.gov>, checks presented for payment are scanned and converted into electronic debits. The electronic debit, rather than the check, is used to collect the funds. Under these rules, agencies are permitted to utilize check conversion at a checkout line or at a lockbox that receives mailed remittances.

These rules currently do not permit agencies to convert other negotiable instruments, such as money orders, traveler’s checks, certified bank checks, and credit card checks. Several agencies have informed FMS that allowing the conversion of these negotiable instruments would facilitate efficiency and improve cash management on their behalf, since these agencies handle many of these instruments on a daily basis. In order to promote efficiency in collections and improved cash management, FMS is proposing to permit the conversion of other negotiable instruments.

The proposed rule also includes modifications to the ACH payment rules. For example, FMS is proposing to require financial institutions to notify Federal agencies when payments are misdirected to an erroneous account because the payment file includes an incorrect account number. This can occur, for example, if a payment recipient mistakenly provides an incorrect account or routing number. Currently, some financial institutions do not notify agencies when a payment is misdirected to an incorrect account. When this approach is taken, the agency that originated the payment is unaware of any problem; therefore, the agency may continue to direct subsequent payments to the wrong account.

After the 90-day comment period, FMS will consider the comments it receives and after analyzing the comments will issue a final regulation. To view the proposed rule, please visit www.fms.treas.gov/ach.

Notifications of Change Provides Easy Fix to EFT Payments

Notification of Change (NOC) is a method used by a financial institution to notify a Federal agency to correct or change account information in an entry the Federal agency processed through the ACH. In certain circumstances, a financial institution may receive a payment file with erroneous information on it, however, it is able to identify the payment and post it to the correct account. In such cases, the financial institution issues a NOC. A financial institution may also issue a NOC when it merges with another bank and a change in account numbers results.

NOCs are used for Federal government (both civilian and military) payments that are made on a recurring basis. Examples are:

- Benefit Payments
- Department of Veteran Affairs
- Office of Personnel Management
- Railroad Retirement Board
- Social Security Administration
- Supplemental Security Income

Other Payment Types

- Federal salary
- *Treasury Direct*
- Vendor and miscellaneous

NOCs should not be used to change title/ownership of an account, change interest of the recipient or beneficiary in the account, change accounts from one financial institution to the other, or for one time payments, such as an IRS tax refund. In these circumstances, a new enrollment form must be processed back to the paying agency.

In many cases, federal agencies do not react timely to NOCs sent by financial institutions. This may result in erroneous payments in the future in which a benefit recipient would experience significant delay in receiving his or her benefit payment, and some beneficiaries depend on these payments arriving timely. Agencies should make every attempt to correct payment files as timely as possible when an NOC is received in response to the payment. For more information on what NOC codes signify, please visit the website at <http://www.fms.treas.gov/greenbook>.

In some cases, financial institutions send NOCs to Federal agencies in an incorrect format. In such cases, financial institutions will receive a refused NOC code that specifies the error in the NOC file. A list of refused NOC codes is also listed in the Green Book at <http://www.fms.treas.gov/greenbook>.

Refused NOCs may also result because third-party payment processors utilize applications that eliminate data from key fields in the NOC file. If a financial institution is using a third-party payment processor for its EFT payment activity, it should contact the processor and ensure that they refrain from eliminating key data in the NOC file.

NOCs take advantage of the electronic ACH system to provide a quick and efficient way to remedy erroneous electronic payments. Both financial institutions and Federal agencies should ensure that they are using NOCs correctly and to the fullest extent to provide the best service to Government payment recipients. If any institution or agency has a question regarding NOCs, please contact Mildred Jones at (215) 516-8170.