

NAME OF SYSTEM: PAPER CHECK CONVERSION OVER-THE-COUNTER

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, the system contains individual information that is contained on the check image which is stored in the system database. Individual information can also be included in a user defined field that is also stored in the system database.

**a. Is this information identifiable to the individual¹?
(If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed.)**

Yes, depending on the information captured by the Federal agency in the user defined field. Also, the digital image of the individual check could contain identifiable information depending on what is contained on the physical check.

**b. Is the information about individual members of the public?
(If YES, a PIA must be submitted with the OMB Exhibit 300 and the IT Security C&A documentation.)**

Yes, the Federal agencies that operate this program only process information about the individual members of the public.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process but is not required to be submitted with the OMB Exhibit 300 documentation.)

No, only individual members of the public.

2) What is the purpose of the system/application?

¹ “Identifiable Form” - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

The Paper Check Conversion Over the Counter (PCC OTC) program converts paper checks received into electronic debits to check writer's account through the Automated Clearing House system, or into a substitute check image that is truncated and cleared under the authority of Check 21. PCC OTC fully automates and improves the collection, reconciliation, research, and reporting processes associated with Federal agency over the counter check collections.

3) What legal authority authorizes the purchase or development of this system/application?

Commissioner Richard Gregg sent a letter dated April 18, 2001, to Patrick Baron of the Federal Reserve Bank of Atlanta requesting he designate a Federal Reserve Bank to act as a fiscal agent of the Treasury for the conversion of checks received in payment for U.S. Government services or products. Based on work the Federal Reserve Bank of Cleveland had been providing for ACH Debit processing, Mr. Gregg suggested it may be beneficial to have FRB-C designated for this activity. The PCC OTC application has undergone a stringent C&A process, resulting in approval of full authority to operate (ATO). The ATO was signed by Nancy Fleetwood, Assistant Commissioner and Chief Information Officer, Information Resources, on June 7, 2005. PCC OTC also operates under the System of Records Notice (SORN) .017 for collections.

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Agency users, FRB-C users, FMS users.,

2) What are the sources of the information in the system?

The digital image of the physical check submitted by the individual member of the public along with the information contained in the user defined fields.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The source of the information is provided by the individual.

b. What Federal agencies are providing data for use in the system?

There are currently 31 Federal agencies providing data for use in this system.

c. What State and local agencies are providing data for use in the system?

There are no state or local agencies providing data for this system. The system is for Federal agencies only.

d. From what other third party sources will data be collected?

No data will be collected from any third party source.

- e. **What information will be collected from the employee and the public?**
Information will only be collected from the public and not employees. The public will submit checks to Federal agencies and the Federal agencies will process those checks into the PCC OTC system.

3) Accuracy, Timeliness, and Reliability

- a. **How will data collected from sources other than FMS records be verified for accuracy?**

No data outside of FMS records is collected into the PCC OTC system.

- b. **How will data be checked for completeness?**

There are image quality edits that aid in capturing a clean check image, which is used to ensure the data needed for check conversion is captured and complete.

- c. **Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

The Federal agencies using the system are required to maintain up to date internal operating procedures which should have steps in place to verify the data is current.

- d. **Are the data elements described in detail and documented? If yes, what is the name of the document?**

Non applicable

D. ATTRIBUTES OF THE DATA:

- 1) **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

All of the data collected by the system as previously detailed in this document is relevant and deemed necessary for the purpose of converting paper checks into electronic transactions. The PCC system is designed to capture the information from the Magnetic Ink Character Recognition (MICR) line of the physical check for check conversion. The MICR line provides the only direction to the pertinent financial information in order to have the check converted. Without the necessary data from the MICR line, check conversion can not occur.

Additionally, information provided to PCC by agencies will only be used as required by that agency.

- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

The system will maintain the data for the sole purpose of check conversion and creating an electronic transaction. New data is created consisting of customers' check writing history. The process of creating new data is created when an ACH debit is returned back to the agency from the FRB. The FRB ACH software, US Dataworks, will transmit a file of return items to the MVD. The MVD will create a record in the system to the specific agency that the transaction was processed. The record is transmitted to the point of sale location and stored on the local verification database. The new data on the local verification database is queried against each subsequent transaction at the point of sale. If the system finds an existing record, then the transaction is not processed unless a supervisor approval is obtained.

3) Will the new data be placed in the individual's record?

If the new data meets certain established criteria by the agency then it is possible that new data can be placed in the individual's verification record. The new data in the verification record is used at the front end when accepting checks through the point of sale system.

4) Can the system make determinations about employees/public that would not be possible without the new data?

If the agency participates in the verification portion of the PCC system, determinations regarding the check writer's check cashing privileges will be made using the new data. Depending on the agency's check cashing policy, the new data can be configured and tailored to meet the specific agency needs. The system will make a determination to process a check based on the agency needs and the new data in the verification record.

5) How will the new data be verified for relevance and accuracy?

The new data will be made available to the cashier and customer at the point of sale and verified by a manager through research. The system has an override feature that allows for the supervisor to force through a transaction that is denied because of the verification system. The agency can connect to the MVD and research all the negative records that belong to their agency. The system employs a number of ways to verify the accuracy of the new data. PCC OTC has system edits to check for accuracy in the configurable fields. There is also an "edit check" feature that verifies the physical check is in the correct ANSI format.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

If agencies choose to share information on the verification database, the system access controls will still be applicable. The agency users will only have access to view the data belonging to their specific location to include the consolidated data from the shared agency. The Paper Check Security document details the strong system controls that are in place to protect the data from unauthorized access.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Not applicable

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

The most efficient means to retrieve data is by using the Item Reference Number (IRN). The IRN is a unique number assigned by the check scanner and follows each transaction through the entire PCC process. According to agency specific requirements, data may also be retrieved by using other agency specific information that is captured at the point of sale. Data may be retrieved by logging on the CIRA search screen and entering the search information. The CIRA will display all the corresponding records in the database for the particular search requested.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

There are no reports that can be run solely on an individual.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Individuals have the opportunity to opt out of having their check collected and the corresponding information made available to the agency by not submitting their check for collection at the point of sale. Individuals that submit their check through the mail can opt out of ACH check conversion. ACH opt out rules are stated in NACHA ACH rules Article two subsection 2.1.4.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The data will be stored in one central site on the internet (CIRA). Data will be collected from more than one site but not accessible to the local site, only on the CIRA.

2) What are the retention periods of data in this system?

The data will be retained for seven years in the PCC system but may vary based on agency requirements.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Procedures for the elimination of data at the end of the retention period are documented in FMS policy S-0200.23. The PCC OTC follows all mandated guidelines in accordance with the policy.

4) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes, the PCC system will be using new technologies to provide: check conversion, check imaging and storing, and automated reporting. PCC will employ Secure Sockets Layer (SSL), Simple Object Access Protocol (SOAP) technology, digital certificates for authentication, and 128 bit encryption.

5) How does the use of this technology affect public/employee privacy?

The public is assured that a high degree of security is associated with Paper Check Conversion transactions, and that appropriate controls are in place to mitigate susceptibility to identify theft, hackers, phishers, and other compromises of their personal and bank account information.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The system does not allow access to users from the general public. However, the system administrator and end users (Agencies) have system access. The system utilizes audit logs to track end users. The audit log will display all user activity within the system. The audit log is an adequate tool used to monitor agencies use of the system.

7) What kinds of information are collected as a function of the monitoring of individuals?

None, the information is only used for the processing of the actual item and is not used for any monitoring purposes.

8) What controls will be used to prevent unauthorized monitoring?

Separation of duties exists at the POS level. The cashier does not have the access to view the MVDB or the CIRA. Refer to the PCC Configuration Management Plan for outline of controls.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

The PCC OTC system is covered under the Systems of Record Notice published for collection systems for Treasury/FMS on February 4, 2003, at 68 FR 5691. The number this Systems of Records Notice is published under is Treasury/FMS.017.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No, the PCC OTC system will not be modified to perform in a manner beyond what has been stated in this document.

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

The user who signs onto the system and the manager are the only individuals who will have access to the data before a batch is transmitted. Once a batch is successfully transmitted to the CIRA, all the data is deleted and not accessible. The financial information is made available to only the agency that processed the transaction.

The FRB-C, FMS's Fiscal Agent responsible for the day to day operations of the PCC OTC system, and their contractor, have access to all data, images, records, and reports. FMS program officials also have access to the data.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

User access to the data is determined by an administrator in the agency who validates and approves the users' role and responsibilities. There are different roles and responsibilities and these translate to various levels of data access. The user role and responsibilities are first authorized then authenticated by the PCC OTC security provisioning model.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

No. Agency users will be assigned roles that restrict access to specific functions within the system.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials.)

The PCC System has several controls in place to adequately prevent the misuse of data. The system has a maximum number of password attempts allowed before being suspended from the system. The Intrusion Detection System will send alerts for suspicious activity. Audit logs are maintained that track each user activity throughout the System. The System has a maximum length of time a user can be idle on the system before being disconnected.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors are involved with the design, development and maintenance of the PCC system. Nondisclosure and confidentiality clauses are a part of their contract.

6) Do other systems share data or have access to the data in the system? If yes, explain.

No other systems share data or have access to the data in the PCC system. The PCC system does not interface with any other systems.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The PCC program manager and information system security officer have responsibility for ensuring compliance.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No. State, local and private/non-federal agencies will not share or have access to the data in the PCC system.

9) How will the data be used by the other agency?

Not applicable.

10) Who is responsible for assuring proper use of the data?

In accordance with TD P 25-07, the PCC OTC program manager is responsible for assuring the proper use of all data collected through and maintained by the PCC OTC application.