Financial Management Service

Privacy Impact Assessment

The Financial Management Service (FMS) Mission is to provide central payment services to Federal Program Agencies, operate the federal government's collections and deposit systems, provide government-wide accounting and reporting services, and manage the collection of delinquent debt owed to the government.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html

Document Date: September 16, 2011

Document Version: 1.1

Name of System: Over The Counter Channel Application (OTCnet)

SYSTEM GENERAL INFORMATION:

1) System Overview: Describe the purpose of the system.

The OTCnet project streamlines and enhances the systems and services FMS provides to support $140 billion annually in federal agency collections transacted at Point of Sale (POS) locations worldwide. The OTCnet application replaces two legacy systems, Paper Check Conversion Over the Counter (PCC OTC) and Treasury General Account Deposit Reporting Network (TGAnet). OTCnet simplifies and modernizes the former OTC revenue business line into a browser-based retail business model that allows FMS to eliminate redundancies within the channel, improves straight-through processing of collections, reduces its operating expenses and increases the security and control of OTC transaction activities.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.

The OTCnet application 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.

3) If the system is being modified, will the SORN require amendment or revision?

__yes, explain.

_x no

4) Does this system contain any personal information about individuals?

x_yes

__no

a. Is the information about members of the public?

Yes.

b. Is the information about employees or contractors?

Yes.

5) What legal authority authorizes the purchase or development of this system?

FMS has unique statutory authority to appoint financial institutions (including but not limited to commercial banks and federal reserve banks) to be financial or fiscal agents of the government. See, e.g., 12 U.S.C § 90. Once appointed, a financial agent "shall perform all such reasonable duties . . . as may be required of them" to support FMS' mission. In this instance, FMS conducted a Financial Agent Selection Process ("FASP") in 2008 that resulted in the selection of Citibank, N.A. ("Citibank") to be FMS' financial agent for the operation, maintenance and development of the Over-the- Counter Channel ("OTCnet")

application. The terms and conditions of Citibank's duties are outlined in the Financial Agent Agreement ("FAA") between Citibank and FMS that was signed and effective on August 28, 2008.

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
   Check all that apply:
   _x Employees
   _x Contractors
   __ Taxpayers
   _x Others (Members of the public, FRB-C settlement gateway and Financial Institutions)

2) **Identify the sources of information in the system**
   Check all that apply:
   _x Employee
   _x Public
   _x Federal agencies
   __ State and local agencies
   __ Third party

   a. What information will be collected from employees or contractors?
   The system contains end-user information about federal employees as they are end-users of the system for processing deposits and checks.
   b. What information will be collected from the public?
   c. Information will collected from the public. The public will submit checks to Federal agencies that will then, process those checks into the OTCnet application.
   What Federal agencies are providing data for use in the system?
   There are currently 7 Federal Agencies using the Check Capture and Processing functions and 66 Federal Agencies using the Deposit Processing functions of the system.
   d. What State and local agencies are providing data for use in the system?
   There are no states or local agencies providing data for this system. The system is only for Federal agencies.
   e. From what other third party sources will data be collected?
   No data will be collected from any third party source.

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 OTCnet application.
   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. OTCnet utilizes the FMS enterprise- wide solution for user provisioning to ensure

that appropriate roles and responsibilities are assigned to OTCnet users, thus providing oversight on OTCnet user access and privileges. For the deposit reporting functionality, accuracy is ensured by deposit preparation being performed by agencies, and deposit confirmation being performed by Financial Institutions.

c. What steps or procedures are taken to ensure the data is current?
The Citi Team performs end user re-certification in conjunction with agencies and financial institutions on annual basis. Data retention standards and polices will be adhered to and monitored by the OTCnet Project Manager.

d. In what document(s) are the data elements described in detail?
The OTCnet data elements are described in the OTCnet data dictionary documentation.

ATTRIBUTES OF THE DATA:

1) How 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 purposes of converting paper checks into electronic transactions. The OTCnet application 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 cannot occur. The data collected by the system is also relevant and necessary for the purpose of collecting, maintaining and sharing information related to OTC transactions performed by participating agencies wherein OTC funds are deposited on behalf of the US Treasury. The OTCnet deposit processing data is at the summary level and doesn't include PII (Personally Identifiable Information).

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? 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 that consist of customers check writing history. New data is created when an ACH debit is returned back to the agency from the FRB via the settlement gateway. The Master Verification Database (MVD) will create a record in the system for the specific agency where the transaction was processed. The agency specific MVD records will be available at the check capture site in order to validate the check writer's history. The subset of data specific to an agency is recognized as the local verification database. The local verification database is queried against with each subsequent transaction at the check capture site. If the system finds an existing record, then the transaction is not processed unless a supervisor approval is obtained. Since the deposit processing information is captured at the summary level, it doesn't contain information at the individual level.

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 verification record is used by OTCnet when accepting checks.

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

If the agency participates in the verification portion of the OTCnet application, then determinations regarding the check writer's check cashing privileges will be made using the new data. Depending on the agency 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 of OTCnet 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 view 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. OTCnet 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?

Access controls requiring user identification and authentication (user name and password) are currently in place to protect the system from unauthorized access. Additionally, 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.

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

Yes. Although the applications used for different processes are being consolidated the processes supported by these applications are not. The consolidation of the applications requires the implementation of security controls to prevent unauthorized access. OTCnet access controls restrict access to OTCnet resources. Internal application access controls are also used to ensure that within the OTCnet application an authenticated and authorized user may only access those system features and functions to which they are entitled.

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

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 check management 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 Central Image Research Archive (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 kind 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)? How can individuals 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.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) What are the retention periods of data in this system? How long will the reports produced be kept?

The data will be retained for 7 years in the OTCnet application.

2) What are the procedures for disposition of the data at the end of the retention period? Where are the disposition procedures documented?

Procedures for the elimination of data at the end of the retention period are documented in FMS policy standard S 210, which OTCnet follows.

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

The online system's user management and functional processes are centralized, ensuring the consistent use of the system and data. The offline system employs centralized user management; data and control data for the offline system is reconciled after being synchronized with the main system, ensuring consistent use of the data.

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

Yes. Java DB and Jetty was used in the implementation of OTCnet to provide embedded application and database servers capabilities

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

The public is assured that a high degree of security is associated with OTCnet transactions, and that appropriate controls are in place to mitigate susceptibility to identify theft, hackers attack attempts, phishing attempts, and other potential compromises of their personal and bank account information.

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

No. 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 activities in the system. 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 kind of information is collected as a function of the monitoring of individuals?**

None. The information is collected as a function of audit log capability of the system and not the monitoring of individuals.

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

Separation of duties exists within OTCnet. The OTCnet access controls restrict access to OTCnet resources using user roles. Internal application access controls are also used to ensure that within the OTCnet application an authenticated and authorized user may only access those system features and functions to which they are entitled.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
Check all that apply:

_x Contractors
_x Users
__ Managers
__ System Administrators
__ System Developers
__ Others (explain)_____

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

The user access to OTCnet is first approved at the participating agency's organization level via a user access application process. The user access to the data is determined by an administrator in the agency who validates and approves the users' role and responsibilities.

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

No. The access of participating agencies' users is restricted to specific functions and specific data within the system within each agency.

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 OTCnet application has several controls in place to adequately prevent the misuse of data including:

- The system accounts have a maximum number failed logon attempts after which accounts are suspended
- The system is protected an Intrusion Detection system that sends alerts of suspicious activity.
- Audit logs related to user activity are maintained and reviewed
- Security training is provided for users and support personnel
- The system has a maximum length of time a user can be idle on the system before being disconnected.

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

Contractors are involved with the design, development and maintenance of the OTCnet application. Non disclosure and confidentiality clauses are a part of the contract.

6) Do other systems share data or have access to the data in the system?

_xyes
__no

If yes,

a. Explain the interface.

The OTCnet is interconnected and/or shares information with following systems:

- Queue Interfaces (DDS: Deployable Disbursing System): Used for providing data to the DDS Interface.
- DTN Webservice: Used by Internal Revenue Service to retrieve the summary or detail deposit ticket information. (IRS) special agency
- Debit Gateway: OTCnet forwards check and transaction information for settlement.
- Client Gateway: Used by offline check capture client to transmit checks information and process batch acknowledgement from special agencies such as IRS, DeCA and Department of Forestry Services (DFS).
- FRB CA$HLINK: OTCnet submits electronic deposit ticket and returned item adjustments to the Federal Reserve Bank's Treasury's cash concentration application – FRB CA$HLINK.
- TRS: Serves as a centralized repository containing of all revenue collection transactions processed by FMS systems. OTCnet currently sends the Deposit Processing transactions to TRS
- System to System Interface Vouchers to FI (Bank of America): Automatically sends the submitted deposits to the Financial Institutions
- National Park Service (NPS) Extract: Used to extract daily deposit and adjustment data as input to agency accounting applications.

- SAM: Used by Deposit Processing to validate Agency Location Codes (ALC) and Treasury Account Symbols (TAS)
- TWAI UDS: Used for reports requiring user information.
- Foreign Currency Service: Used by OTCnet to retrieve foreign currency rate during Foreign Cash Deposit creation, and in the process for confirming Foreign Check Item Deposits.
- ITIM : Used to control User Authentication and Authorization. Utilizes the OTCnet AGM function to assign roles to users.

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.

The OTCnet Business Owner has the responsibility for ensuring that the system complies with applicable privacy law and regulation.

7) Will other agencies share data or have access to the data in this system?

x_yes
__no

If yes,

a. Check all that apply:

_xFederal
__State
__ Local
_xOther (explain) _____

The OTCnet is interconnected and/or shares information with:

- National Park Service
- Bank of America (system-to-system interface for deposits)
- Foreign Currency Conversion Service (Bank of America)
- Internal Revenue Service
- DDS
- IRS
- SAM
- TRS
- ITIM
- UDS
- Debit Gateway

b. Explain how the data will be used by the other agencies.

The data is used by the agency for their deposit and check processing activities. For the above agencies (NPS, IRS, and DDS), specialized interfaces have been developed to allow for the OTCnet application to interact directly with their internal deposit or check processing systems. The Federal Reserve Bank of Cleveland via the Debt Gateway utilizes the data received by OTCnet to settle the check items that have been captured by OTCnet.

c. Identify the role responsible for assuring proper use of the data.

In accordance with TD P 25-07, the OTCnet Business Owner is responsible for assuring the proper use of all data collected through, and maintained by the OTCnet application.

FMS Privacy Impact Assessments (PIA) http://www.fms.treas.gov/pia.html