The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service is to promote the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, payments, and shared services.

This Privacy Impact Assessment is a Public document and will be made available to the general public via the Fiscal Service Privacy Impact Assessment (PIA) webpage (shown below).

Fiscal Service - Privacy Impact Assessments (PIA):
http://www.fiscal.treasury.gov/fsreports/rpt/fspia/fs_pia.htm

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

Document Version: 1.5

Document Date: August 1, 2017

SYSTEM GENERAL INFORMATION:

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

The OTCnet application helps Fiscal Service achieve improvements in cash management operations, collection mechanisms, and systems consolidation. The OTCnet project streamlines and enhances the systems and services Fiscal Service provides to support billions of dollars annually in federal agency collections transacted at Point of Sale (POS) locations worldwide.
OTCnet streamlines and modernizes this environment by transforming the OTC revenue business line into a browser-based retail business model that allows the Fiscal Service to eliminate redundancies within the channel, improve the straight-through processing of collections, reduce its operating expenses, and increase the security and control of OTC transaction activities. By consolidating existing systems and expanding their functionality, the application provides federal program agencies and banks with a single source of OTC information.

The OTCnet application consists of the following components:

Deposit Processing Module

The Deposit Processing module provides Financial Institutions (FIs), Federal Program Agencies (FPAs), and Federal Reserve Banks a secure web-based system for federal agency deposit reporting and confirmation. Allowing users to enter not only summary deposit information that is required on the SF 215 Deposit Ticket, this module also provides cash consolidation capabilities by allowing deposit information to feed their administrative accounting systems for the US Treasury's general account and allows participating agencies and financial institutions to quickly confirm deposits. Additionally, agencies can monitor the status of their deposits as they proceed to the FI and obtain reports on their associated deposits. Thus providing, Fiscal Service and the FPAs with near real-time visibility into the accounting data for OTC collections.

On-line Check Capture and Processing Module

The On-line Check Capture and Processing module provides a cost-efficient alternative to paper check processing by facilitating check processing at the point of sale via web enabled interfaces. This module converts paper check into a digital representation (images and data) and provides electronic and automated check processing, validation, and debit/credit of funds.

Off-line Check Capture Module

The Off-line Check Capture module provides a cost-efficient alternative to paper check processing by facilitating check processing at the point of sale when the Off-line Check Capture module is not connected to the real-time processing mechanisms of the OTCnet application. This module converts paper checks into digital representations (images and data) and provides electronic and automated check processing, validation, and debit/credit of funds. The off-line Check Capture module communicates with the On-line module through a XML Gateway and web services.

OTCnet Local Bridge

The OTCnet Local Bridge (OLB) is an application that will be required and installed with the Websocket based architecture on all terminals performing check processing and terminal configuration operations. The OLB serves as a bridge between the workstation and browser for the following functionalities: Check Scan (Online/Offline), DDS Transmission (Online/Offline) and Terminal Detection (Online/Offline).

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

Treasury/FMS.017- "Revenue Collections Records"

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 ofthe public? Yes

b. Is the information about employees or contractors? Yes

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

See, e.g., 12 U.S.C § 90.

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
_X_Employees
_X_Contractors
_X_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?**

Information will be collected from the public. The public will submit checks to Federal agencies that will then, process those checks into the OTCnet application.

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

There are approximately 100 federal agencies using the Check Capture and Deposit Processing functions of the system.

d. **What state and local agencies are providing data for use in the system?**

None.

e. **From what other third-party sources will data be collected?**

None.

3) Accuracy, Timeliness, and Reliability

a. **How will data collected from sources, other than Fiscal Service records, be verified for accuracy**

For the deposit reporting functionality, accuracy is ensured by the deposit preparation performed by agencies, and the deposit confirmation performed by Financial Institutions. .

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 Fiscal Service 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?**

End user re-certification is performed 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) creates 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., in such cases 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?

All data maintained by this system is retained and destroyed in accordance with the Fiscal Service File Plan. All records schedules and categories within the Fiscal Service File Plan are approved by NARA.

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

After the retention period, the Assistant Commissioner for Revenue Collections Management must send a memo to the Chief Counsel through the Assistant Commissioner for Management, with a description of the data to be destroyed, along with a proposed method of disposition. Specific procedures are outlined in the TWAI Data Retention and Disposition guidelines.

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 Fiscal Service has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes, embedded application and database server capabilities were used in the implementation of OTCnet.

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.

7) What kind of information is collected as a function of the monitoring of individuals?

None.

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 with 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?

_X_ yes
____no

If yes,

a. Explain the interface.

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

- Queue Interfaces Deployable Disbursing System (DDS): Used for providing data to the DDS Interface. Accounting code information (including the C- Key / TAS String) is submitted along with the check information being submitted from both Online and Offline modules.
- DTN Webservice: Used by Internal Revenue Service to retrieve the summary or detail deposit ticket information.
- Debit Gateway: OTCnet forwards check and transaction information for settlement.

- Client Web Interface: Used by online and offline check capture client to transmit checks information and process batch acknowledgement from certain agencies such as IRS, DeCA and Department of Forestry Services (DFS).
- Treasury Cash Management System (TCMS): Serves as a centralized repository containing of all revenue collection transactions processed by Fiscal Service systems. OTCnet currently sends the Deposit Processing transactions to the Collections Information Repository (CIR).
- 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.
- Shared Accounting Module (SAM): Used by Deposit Processing to validate Agency Location Codes (ALC) and Treasury Account Symbols (TAS). This handles the validation of up to 1,000 TAS Strings for validation at one time.
- 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. ITIM also uses TWAI UDS which is used for reports requiring user information.

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:

_X_Federal
____State
____ Local
_X_Other (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
- SAM
- Collections Information Repository (CIR)
- 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 (FRB)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.

The OTCnet Business Owner is responsible for assuring the proper use of all data collected through, and maintained by the OTCnet application.