The Bureau of the Fiscal Service

Privacy Impact Assessment

The mission of the Bureau of the Fiscal Service (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: PACER On-Line (with) Digital Check Imaging (POL)

Document Version: 1.1.2

Document Date: 1/23/2017

SYSTEM GENERAL INFORMATION:

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

PACER On-Line (POL) functions as an on-line shared database that supports the Bureau of the Fiscal Service Regional Financial Centers' (RFC) accounting and claim processes. The application provides daily check reconciliation, daily electronic fund transfer reconciliation, daily accounting balancing and cancellation information. POL functions include: Inquire on payment information, Submit claim requests, Request, display, print check images, Submit and retrieve accounting information. POL batch functions include processing: Claim requests files, Accounting files; Electronic fund transfer returns files, Check return files, Payment data files. POL reports and forms include: Daily check reconciliation, Daily electronic fund transfer reconciliation, Daily accounting balancing and Cancellation information.
The Digital Check Imaging (DCI) module allows users to request, retrieve, view, and print all digitized U.S. Department of the Treasury (Treasury) checks that have been processed by the Federal Reserve Banks (FRB) and have been captured and archived by the Federal Reserve System (FRS). The RFCs also use DCI to scan reclamation documentation in support of POL claims and accounting processing. In addition, the system is used to match images with Claims Documentation.

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

Treasury/FMS .002 Payment Records,
Treasury/FMS .010 Delegations and Designations of Authority for Disbursing Functions

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 – there is information used to make federal government payments to a person that may include name, address, amount(s) and banking account information.**

   b. **Is the information about employees or contractors?** Yes – employees and contractors may be included.

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

- See, e.g., 5 USC 301; 31 USC 3325 and 31 USC 3321, note; Executive Order 6166, dated June 10, 1933.

- In addition, 31 CFR part 240 governs the endorsement and payment of checks drawn on the United States Treasury. *See, e.g.,* 31 CFR 240.6(c)(2)(authorizing Treasury to decline payment on any Treasury check bearing forged or unauthorized endorsement). The Competitive Equality Banking Act of 1987, Public Law No. 100 – 86, Title X, establishes time limits for payment on stale Treasury checks and claims on stale Treasury checks, and authorizes Treasury to prescribe rules, regulations, and procedures necessary to implement the pertinent provisions.

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 (describe) Payees/Recipients of US Government Payments**

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

   a. **What information will be collected from employees or contractors?** None

   b. **What information will be collected from the public?** None

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

   All Federal Program Agencies (FPA) for which Fiscal Service provides disbursing services (i.e., almost every Federal agency), submit data to the Regional Financial Centers. Also the Federal Reserve System provides the various images.

   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?**

There is no data collected from sources other than Fiscal Service. Payment data comes only from RFCs. Each RFC is responsible for the accuracy of the payment data submitted, not PACER. PACER receives Check detail and Status information, cashed or not cashed, from the Treasury Check Information System (TCIS). Fiscal Service maintains no files as to entitlement for any recipient of a payment. Fiscal Service issues at the request of a FPA.

b. How will data be checked for completeness?

PACER enforces file format edits, but cannot check the data for completeness. Fiscal Service payment applications validate the data for completeness to make a payment. The DCI customer will verify that the digitized check image requested contains the correct name, amount, check symbol serial number, signature and various bank stamps on the back of the digitized check image. However, this only occurs when a claim has been placed and is being researched.

c. What steps or procedures are taken to ensure the data is current?

PACER receives payment information files every day from the RFCs with current data. PACER compares the check ranges to ensure all data is in sync. Reports are generated if any data is missing. Support personnel notify the RFCs if daily files are not received.

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

The Computer Program Specification Series (CPSS) is a database of specifications that describe and outline the data elements of various file formats processed by PACER.

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?**

   PACER was designed to perform accounting, claims and cancellations against payments issued through the RFC. The detailed payment data is essential to be able to perform those functions. In addition it allows users to view details of the payments that their agency has requested so they may perform claims and inquiry processes. DCI allows them to view images of negotiated checks for the same purpose.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?** No
   How will this be maintained and filed? N/A

3) **Will the new data be placed in the individual's record?** N/A

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

5) **How will the new data be verified for relevance and accuracy?** N/A

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

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

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.)**

   Payment data can be retrieved from the PACER database by a payment identifier of the payee or at the individual payment detail level, check or EFT. Digital check images and supporting documentation are requested by an authorized user via PACER module. The images are ordered from the Federal Reserve System and are downloaded to the DCI database.

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

   All payment data is collected at the detail level, however the system is not designed to generate reports on the payment data of individuals. By accessing PACER On-line, an authorized user can view individual payment records. Access is restricted by FPA (i.e., a user can only view data for the Agency Location Code (ALC) for which they are authorized). No reports are produced on individuals.

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?**

   N/A – All data is passed directly from the RFCs to PACER.

   Individuals are not involved because information on a payment comes to PACER from the Financial Centers that work with the Federal agencies. Individual involvement is at the agency level.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

   Data is retained in PACER indefinitely. Reports go to an archival and retrieval system that stores computer output such as reports. The normal retention period for reports is 12 months.

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

   As indicated above, all payment data in PACER is maintained indefinitely. Check images are purged after 60 days. The number of days can be increased or decreased at the discretion of Fiscal Service management. PACER has a legal requirement to retain scanned documents for an indefinite period of time.

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?**

   PACER is a major application. All users run the same version of the application. Fiscal Service configuration management procedures permit only one version to be in production at any given time.

4) **Is the system using technologies in ways that Fiscal Service has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?** No

5) **How does the use of this technology affect employee or public privacy?** N/A

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

7) **What kind of information is collected as a function of the monitoring of individuals?** N/A

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

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
      _x Contractors
      _x Users
      _x Managers
      _x System Administrators
      _x System Developers
      _x Others (explain) Production Support Personnel

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

   Access request forms are required to gain access to PACER. They are documented in databases controlled by Fiscal Service. Each FPA end user is programmatically restricted to view and process data only for his/her own agency as specified by the agency. Access is strictly on a need to know basis. All users at a given FPA can view specific payment data for that FPA. Fiscal Service users at RFCs can view payment data for all FPAs serviced by them. A user with access to PACER will also have access to DCI modules although the agency determines who can view check images. Criteria, procedures, controls and responsibilities regarding access are documented in the PACER System

Security Plan. Criteria and controls are contained in PACER documentation. Procedures and responsibilities are contained in user manuals and PACER Rules of Behavior. These Rules of Behavior must be accepted yearly or the user cannot access POL.

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

PACER users are restricted to only the functions they need to perform their duties. For example, regular users cannot access the system audit logs. User level of access is authorized and reviewed to ensure that the user access does not exceed position requirements. External users are further restricted to only see the data that they have issued. Therefore, a Social Security Administration user cannot see Internal Revenue Service data.

The user's access to DCI data is restricted. A user will only be allowed to access digitized check images and supporting check documentation based on their ALC.

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 following controls are in place to prevent the misuse or unauthorized use of data by those having access include:

- The principle of least privilege is applied by restricting access on a need-to know basis
- Fiscal Service limits the number of login attempts by a user during specific time limits
- Access enforcement includes individual accountability and audit trails where passwords are associated with a user ID that is assigned to a single individual
- Access Control Lists are reviewed regularly to identify and remove users who have left the organization or whose duties no longer require access to the application. The regularity depends on the type of user. POL has monthly, quarterly, semi-annually and annually recertification of users and reviews. Daily notifications are sent out for action when an access needs to be removed.

The PACER Rules of Behavior are a primary source of information to identify the various controls in place. They clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules also state the consequences of inconsistent behavior or noncompliance. Fiscal Service has also established a baseline set of Rules of Behavior that all users must read and acknowledge before they are granted access to the application.

In addition, all legitimate users must access PACER via SecureID and their assigned user ID. As explained previously, FPAs are responsible for determining all entitlement to payments they certify. Therefore, PACER grants all users from a given FPA ALC access to data for that ALC unless requested differently.

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?

Yes, standard Privacy Act clauses are included in 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.

   PACER receives and passes data files to and from other Fiscal Service systems, but does not share a database with other internal Fiscal Service systems, or external agencies.

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

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
      __Other (explain) _____

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

   FPAs submit data to RFCs who submit data to PACER. Each FPA has access to its own data. Data is not shared and access is not provided to State, Local, or other agencies.

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