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:
November 11, 2011

Document Version:
Version 1.2

Name of System:
Debit Gateway

SYSTEM GENERAL INFORMATION:

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

The Debit Gateway (Debit Gateway) application and settlement services was created in order to remove item/entry presentment and settlement processes from the collection channels to modernize, streamline, and improve collection processes. The Debit Gateway is an integral component of the Collections and Cash Management Modernization (CCMM) effort. The Debit Gateway:

- Receives check and ACH transaction data from multiple collection channel applications;
- Determines whether to present the transaction as an ACH entry, or as an image check;
- Creates payment mechanism formatted entries and presentment/origination files;
- Delivers entry image cash letters and ACH origination files to FedForward (image check) and FedACH (ACH);
- Processes returned checks and ACH debits;
- Provide check and ACH debit entry settlement data to the channel applications for subsequent reporting.

.

The Debit Gateway application receives check and ACH debit transaction data acquired in the multiple collection channel systems, such as the Internet channel (Pay.gov, EFTPS), the mail channel (ECP), and the OTC channel applications, and clears those transactions through the FedACH and FedForward (Check21) systems. After receiving the transaction data in a standard format from the channel systems, the Debit Gateway reformats the transactional data into the standard ACH and Check format and forwards the file to the FedACH and Check systems for presentment and settlement. The Debit Gateway sends files that report settlement activity to CA$HLINK and the channel applications.

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

FMS .017—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 individual members of the public?

YES

b. Is the information about employees or contractors?

NO

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

The legal authorities applicable to this system are:

5 U.S.C 301 Departmental Regulations
31 U.S.C 321 General Authority of the Secretary
31 U.S/C chapter 33 Depositing, keeping, and paying money
31 U.S.C 3720 Collection of Payments

DATA IN THE SYSTEM:

1) Identify the category of individuals in the system

Check all that apply:

__ Employees

__ Contractors

X_ Taxpayers

X_ Others ((Individuals and Businesses paying for goods, services, fees, or taxes to the Federal Government)

2) Identify the sources of information in the system

Check all that apply:

__ Employee

X_ Public

X_ Federal agencies

__ State and local agencies

X_ Third party

a. What information will be collected from employees or contractors?

None

b. What information will be collected from the public?

The Debit Gateway does not receive information directly from the public, but indirectly through the channel partners. The collection-related information is the account number and financial institution routing number used to present the transaction to the payer's bank for settlement and posting. Individual or company names and addresses may be included on check images, and names and other identifying information will typically be in ACH entries.

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

Many Federal agencies are providing routine check and ACH data for settlement to our channel partners, so data from Federal agencies is received indirectly.

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

None typically.

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

FedForward (Check 21) and FedACH (ACH) send return data to Debit Gateway which contains comparable data to forward collection transactions.

3) Accuracy, Timeliness, and Reliability

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

The Debit Gateway operations staff will have access to channel applications to reconcile data received by the Debit Gateway from each of the channels. The data is verified for accuracy by validating item count and total dollars at various points throughout the day. The same reconciliation is done with the outputs or downstream applications (FedForward (Check 21) and FedACH (ACH).

b. How will data be checked for completeness?

The data is checked for completeness by reconciling the data received by the Debit Gateway with the data sent by each of the channels.

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

Data sent from the channels to the Debit Gateway is typically processed the same day it is received, before the established cutoff time for the particular channel. The data received after the established cutoff time is processed the next day. If the channel sends a late data file, arrangements between the channel and Debit Gateway management are needed to process the late file.

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

The USDataworks Interface Guide and the XML schema document the data elements sent from the channels. It also contains data elements contained in the RPF processing status files sent by the Debit Gateway to the channels. The data dictionary describes all the data elements stored within the Debit Gateway application. The NACHA Rule book describes the data elements contained in the files sent by the Debit Gateway to FedACH. The ASC X9.37 Check21 standard image file format describes the data elements (and image formats) required in the FedForward files.

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?

The Debit Gateway receives check and ACH transaction data from multiple collection channel applications as input. The use of the data provided by the collection channels is relevant and necessary for the Debit Gateway to determine whether to present the transaction as an ACH entry, or as a check image. This data is also relevant and necessary for creating payment mechanism formatted entries and presentment/origination files in a manner that will enable the transactions to settle and post to payer accounts. The Debit Gateway delivers entry files to FedForward (check image) and FedACH for settlement. Debit Gateway processes and settles forward and return transactions and provides check and ACH debit entry data to the channel applications for subsequent reporting to TRS.

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?

No.

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.)**
The data is retrieved using unique sequence numbers assigned to transactions and through criteria on search screens such as process date, Agency Location Code, and dollar range. Personal Identifiers will not be used to retrieve the data.

9) **What kind of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**
None.

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?**
This is applicable to the channel partners, but not to the Debit Gateway. Paying individuals must utilize an acceptable payment alternative (e.g., credit card). Notice of ACH conversion is provided. Those opting out of ACH conversion can so state, resulting in items being processed through FedForward, or use another payment mechanism (e.g., credit card**).**

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 retention periods for Debit Gateway transactions are 60 days of data online and 7 years of data offline (archive). Litigation items are retained indefinitely. Data includes every piece and format that the Debit Gateway receives, stores, and sends.

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

Records in electronic media are electronically erased using industry-accepted techniques. Disposition of data is a common control provided by the General Support System (GSS) as documented in the Debit Gateway Security Plan.

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 Debit Gateway production environment has a primary and an alternate site, alternating between the Consolidation Center 3 (CC3) and the Consolidation Center 1 (CC1). In the event of a primary site failure, Debit Gateway production will be relocated to the alternate site. Data replication, along with additional backups, is used to facilitate the recovery.

4) Is the system using technologies in ways that FMS 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.

Yes, Audit logs are built within the Debit Gateway application to track system user activity.

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

Monitoring capabilities are in place within the Debit Gateway application to determine what data was accessed or changed by system users. The system captures auditable records within a table stored in the database and provides a trace of user actions performed within the application. Debit Gateway logs all activities associated with modifications, entry, and exits. Some auditable records will include "before change values" and change value relating to any modifications made to records. Unauthorized attempts of logins in to Debit Gateway are also captured through Siteminder.

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

Separation of duties is enforced within the application by providing appropriate roles for the administrative user. Unauthorized attempts to log in to Debit Gateway are monitored. The Debit Gateway application has a standard report to identify any unauthorized access and is reviewed by the Application Security function. Debit Gateway users are required to use a two-factor authentication using Siteminder, making it extremely difficult for unauthorized users to access the system**.**

ACCESS TO DATA:

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

__ Contractors
X Users
__ Managers

X System Administrators
__ System Developers
X Others (Debit Gateway Technical Support Staff**)**
System users will only be individuals at FRB-Cleveland. Their user accounts are stored within the LDAP and are part of UPS. The application has the ability to allow access from an external authentication mechanism. An entry matching the external user is used to control the authorization of the user within the application. Two-factor authentication, enforced by Siteminder, is used.
Technical support staff at FRB Cleveland has "read only" access to the Debit Gateway data that resides in files and within Oracle tables in the data tier at the TWAI. This access is needed for troubleshooting and ad hoc reporting. This access is managed and controlled by the GSS.

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

FRB Cleveland using documented formal procedures. All requests for access and account modification are documented electronically, appropriately approved, and retained. Privileges are authorized by FRB Debit Gateway management for the Debit Gateway accounts.
The Debit Gateway uses external authentication, using Siteminder and the User Provisioning System (UPS) provided by the TWAI. FRBC Application Security creates accounts using the UPS application, and within UPS assigns the authorization to use the Debit Gateway. Existing UPS accounts, provisioned by another application like TWAI Central, can also be selected and assigned the authorization. These external accounts are then "linked" to the account within the Debit Gateway application by FRBC Application Security staff.
In addition, the user needs an iKey 2032 USB token or equivalent with the appropriate certificate loaded. The Data Access Control Division (DACD) of FMS is responsible for issuing Debit Gateway certificates and FRBC follows their procedures for obtaining this access.

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

The Debit Gateway has privileges (functions) defined within the application that are assigned to roles. The roles within the application are designed to enforce "least privilege".

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)

New system users are required to read and sign the UPS Rules of Behavior before gaining initial access to Debit Gateway. Since all administrative users are FRB Cleveland, they are also required to sign the FRB Cleveland rules of behavior, and resign it annually. Additionally, the Debit Gateway audit log captures user activity, and it is reviewed to determine if misuse occurs**.**

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, a software vendor (US Dataworks) is involved in the design, development, and testing of the Debit Gateway system. Non-disclosure statements, in addition to a confidentiality clause, are included in the contract agreement.

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 channel applications are the source data for Debit Gateway processing. The transaction information provided by the channel through Connect:Direct is used to settle the transactions. This information is processed and provided to the FedACH and Check21 systems for further processing. Summary information is provided to FRB CashLink in the form of deposit tickets and debit vouchers. Status information is shared back to the channels.

b. Identify the role responsible for protecting the privacy rights of the public and employees affected by the interface.
Each channel is responsible for protecting and securing the privacy of the information contained within their respective systems.

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

__ yes
X no (comments provided below)

If yes,

a. Check all that apply:
__ Federal
__ State
__ Local
__ Other (Channel partner data**)**

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

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