TREASURY

FINANCIAL MANAGEMENT SERVICE

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: June 8, 2011

Document Version: 1.0

Name of System: Stored Value Card (SVC) Program

SYSTEM GENERAL INFORMATION:

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

SVC uses smart card technology with "electronic purses" to eliminate coin, currency, scrip, vouchers, money orders and other labor-intensive payment mechanisms in closed Government locations, such as military bases.

This program is aimed at eliminating the float loss associated with the more than $2 billion in coin and currency in circulation on military bases and other closed Government locations around the world. Stored value cards also eliminate the cost of securing, transporting, and accounting for cash held outside the Treasury. In addition, stored value cards eliminate the manually intensive back-end operations necessary to support scrip, vouchers, meal tickets, money orders, traveler's checks, and other paper payment mechanisms used in closed Government environments.

Stored value cards are issued to military personnel and contractors, including merchants at selected Government sites. The cards may be issued in fulfillment of a Government payment, as is the case at all Army, Air Force and Marine Corps basic military training sites, where soldiers receive their initial payroll on stored value cards. Or, the cards may be issued without value so that cardholders can load funds onto them from their personal bank accounts. For example, at U.S. bases in Honduras, individuals can withdraw funds from their bank accounts in the United States to obtain a credit on their stored value card. Merchant locations on the Government sites, including stores and service providers, are equipped with stored value collection terminals so that cardholders can make purchases with the card.

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

Treasury/FMS.017

Collections Records-Treasury/Financial Management Service

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. Information is about active duty military personnel and military government contractor personnel.

b. Is the information about employees or contractors?
See 4.a. above.

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

5 U.S.C. 301; 31 U.S.C. 321; 31 U.S.C. chapter 33; 31 U.S.C. 3720

DATA in the SYSTEM:

1) Identify the category of individuals in the system
Check all that apply:
__ Employees
__ Contractors
__ Taxpayers
_X_Others (describe) Army, Air Force and Marine Corps basic trainees; deployed military personnel at selected overseas bases and troop transfer stations; civilians (contractors, including commercial/retail salespeople) at selected overseas bases and troop transfer stations.

2) Identify the sources of information in the system
Check all that apply:
__ Employee
__ 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?
SVC collects information from active duty military personnel and military government contractor personnel. Below is a description of the type of information SVC collects:

Social Security Number
First, Middle and Last Name
Banking Information
Mother's Maiden Name
Rank & Title
Date of Birth
Address

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

DFAS, United States Army Finance Command (FINCOM)
Name, address, social security number, telephone number, e-mail address, date of birth for all SVC cardholders. For SVC cardholders who use the Self-Service Kiosks, SVC also collects banking data (routing number, account number, account type).

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?**

Equifax

3) **Accuracy, Timeliness, and Reliability**

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

Information provided by DFAS for all EZpay program participants (basic military trainees) is output for SVC's use from the Military Pay records; this information has been verified by the appropriate service branch.

Information provided by EagleCash participants is input by the local base Finance Officer or their designated cashier(s) and, for military personnel, can be verified against Military Pay records and/or Military ID card (i.e. CAC).

Information provided by Equifax is verified manually. Equifax provides name and address information for individuals who a part of the SVC program debt collection process. The SVC program sends out a "Debt Letter" on behalf of Fed Debt.

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

Information provided by DFAS for all EZpay program participants (basic military trainees) is output for SVC's use from the Military Pay records; this information has been verified as complete by the appropriate service branch.

Information for EagleCash participants is input by the local base Finance Officer or their designated cashier(s); information for military personnel can be checked for completeness against Military Pay records and/or Military ID card (i.e. CAC).

c. **What steps or procedures are taken to ensure the data is current?**
For EZpay, the local Finance Office will send an updated file if information about the cardholder needs to be updated; the same holds true for EagleCash Finance

Officers and cardholders. In addition, EagleCash Self-Service Kiosk users are instructed upon Kiosk enrollment to re-enroll at the Finance Office if their banking data changes. Lastly, if a Self-Service Kiosk user's banking data is determined to be out of date (i.e. transaction is returned via FedACH), the cardholder's card will be locked out of ACH transactions with a message referring the cardholder to the Finance Office, and the local Finance Office is instructed separately to locate the cardholder and obtain up-to-date account information.

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

All data elements are incorporated into database schema diagrams which are available upon request; these database schema diagrams are supersets of data collected from the field – they also include other fields which are system-related but are calculated, used as indices, etc.

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 SVC Program uses the data collect to initiate debit and credit entries to the card holders bank or credit union account. The cardholder completed a DD 2887 form in which authorizes the SVC program to conduct debit and credits to the cardholders account. Its necessary for the SVC program to collect the abovementioned information in order to process a SVC program transaction at any Self Service Kiosk or ACH-based laptop

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 tracks all smart card transactions for the individual cardholders. In this manner, there is additional information created about the cardholder/individual, in terms of their spending pattern while on base. This information is collected automatically, through the "processing" of SVC files received from Point of Sale (POS) devices, Self-Service Kiosks and Finance Office issuance stations/laptops; processing involves FRB receiving, collecting and uploading these transaction files into master databases for each of the two SVC programs. These transactions then create individual database records for each transaction performed; from this, the database can display a history via the back-office only, showing the spending patterns of the individual in question.

This information is maintained electronically in a SQL Server database.

If there is a residual value remaining on the card after expiration, that residual should be returned to the cardholder. This process has been automated for the EZpay program, and this information is sent to DFAS for returning of funds via the Military Pay application. The process is not automated for the EagleCash program, so there is no new data created for these individuals through the residual process.

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

As noted above, residual information is exchanged with DFAS, in order to allow for DFAS to return any outstanding residual value post-expiration to a basic trainee. This information is sent via FedACH. Further, information about whether an SVC cardholder owes a debt as a result of use of the SVC is exchanged with DFAS in order to allow DFAS to collect the debt from the pay of military personnel who owes the debt.

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

N/A. The SVC does not make determinations about employees/public.

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

The data are produced from an automated application which processes all residuals for EZpay in a like manner. Data about is verified manually and by sending notice about the debt to the affected cardholder.

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

The SVC program observes "Least Privileged". All data is restricted based on a user's role and responsibility.. In addition, there are physical and logical controls which prevent any unauthorized access to the server area and the servers/databases themselves.

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

The SVC program observes "Least Privileged". All data is restricted based on a user's role and responsibility.. In addition, there are physical and logical controls which prevent any unauthorized access to the server area and the servers/databases themselves.

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.)**

Information is retrieved by social security number or SVC card number at the direction of an operator, using an SVC Program application on anSVC workstation at the Federal Reserve Bank in Boston. Information may also be retrieved by name. Information can also be displayed using Crystal Reports, or by viewing through a module of the SVC back-office system to only users with authority to view such information.

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

Reports produced include: Card Issuance (initial issuance or subsequent reloading of funds), Transaction History, and Kiosk activity. These reports are used primarily for internal use at the FRB of Boston, either to reconcile a day's processing work or to assist with the research of an outstanding issue with a particular card. Reports are sent to SVC Program Managers, DFAS and to selected program-participating merchants. However, the data shared with these recipients varies (i.e. merchants only receive information about their own activity, not about individuals' issuance activity). In addition, the back-office system is only accessible to a limited number of authorized users from SVC – FRB employees or contractors, as well as an FMS SVC Program Manager.

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 are free to decline providing banking data for EagleCash card issuance; however, declining to provide this information will require that the user forego Self-Service Kiosk enrollment, as the information is required to process any Kiosk ACH-based transactions (i.e. Self-Service Card Load from Bank Account or Self-Service Card Unload to Bank Account). Further, individuals are not required to enroll in the EagleCash program. Upon enrollment for the EagleCash program, individuals sign an enrollment form (DD Form 2887) consenting to the use of their information for the EagleCash program.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

Data are retained indefinitely.

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

N/A

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?**

N/A – the system is only operated in a single site (Federal Reserve Bank of Boston).

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.**

An individual cardholder's transaction history allows for a system operator to review the location and dates/times of purchases over the lifecycle of that particular smartcard. The merchant location (i.e. Bagram AAFES), date and time are recorded in each transaction record and are stored in the central database for that particular smartcard program. However, this data is not real-time; it is based on a time lag inherent in the system (which is offline, with batch processing), so there is no opportunity for real-time monitoring or tracking of individual cardholders.

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

No data is collected specifically for the purpose of tracking or monitoring individuals; all data collected are required for the timely, accurate payment to merchants for sale activity, posting of funding transactions, etc. The ability to track or monitor individuals' purchase patterns (after the fact) is ancillary and may be used on an ad hoc basis by military law enforcement only where there is suspected fraudulent or unauthorized use of the card.

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

Access to the SVC system is limited to individuals authorized specifically for the purpose of completing tasks and work related to SVC transaction processing, settlement or reconciliation (or support thereof). See Access to Data., below.

ACCESS TO DATA:

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

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

The following categories of individuals have access to the back-office system:

- Federal Reserve Bank of Boston (FRB) SVC employees – staff at FRB designated to provide support for SVC processing/settlement/reconciliation, hardware deployment, server infrastructure management, and software development

- FRB contractors – individuals under contract with FRB to provide support for SVC deployments or software testing/development

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

Access is assigned based on the principle of least privilege; rights are assigned at the Active Directory (server/network infrastructure), database and application/function levels, with the smallest possible set of rights provided to each individual – the minimum required for them to perform their assigned duties.

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

User access is restricted, as noted above. Individual cardholders have no access to the system other than to the balance on their card, which is held on the chip and does not require access to the back-end system to determine.

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)**

Each SVC user with access to the back-end system is required to sign a Rules of Behavior document explaining the responsibilities inherent on all users of the system. This document also includes language specifically noting the appropriate disciplinary action for failure to comply with the Rules of Behavior. In addition, all users are undergo Security Awareness Training.

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. All Contractor Contracts Contain a Non-Disclosure agreement.

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

__ yes
_X_no

If yes,

a. Explain the interface.

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

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

yes
_X_no

If yes,

a. Check all that apply:
__Federal
__State
__ Local
__Other (explain) ________________

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

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

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