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 Service: Card Acquiring Service (CAS)

Document Version: 1.0

Document Date: 6/29/2016

SYSTEM GENERAL INFORMATION:

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

Formerly referred to as the Plastic Card Network (PCN), the Card Acquiring Service was established in 1987 and is one of the collection mechanisms that the Fiscal Service manages for federal departments and agencies. CAS is essential to the collection of federal revenue, and processes these transactions in an efficient, timely and cost-effective manner. Federal entities, in the U.S. and abroad, rely on CAS for the acceptance of credit, debit and other payment cards (e.g., Electronic Benefits Transfer – EBT) from customers transacting business at the point of sale, through the mail, via the internet, and over the telephone. CAS supports the major card brands (American Express, Discover, MasterCard, VISA, and regional and national debit networks).

Reflecting the U.S. commercial marketplace, the acceptance environment for federal agencies includes traditional stand-alone terminals, integrated point of sale (POS) systems, mobile applications, kiosks, and Internet-based software applications. CAS receives card transactions from these sources and via the Fiscal Service's Pay.gov internet payment portal. Pay.gov transactions can include transactions from the Fiscal Service's Revenue Collections Management (RCM) Mail channel when credit and debit card information is included on forms sent to RCM's General Lockbox Network (GLN). Funds typically settle on a next-day basis. CAS provides information to RCM's Collections Information Repository (CIR) for agency viewing and reconciliation.

All CAS customer agencies are processing with our current Financial Agent, to fulfill the role of card acquirer/processor to the CAS program.

2) Under which Privacy Act Systems of Records Notice (SORN) does the system operate? Provide number and name.
No SORN is required, N/A

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, the cardholder's account number, known as a Primary Account Number (PAN). The card account number alone cannot be tied back to an individual.

b. Is the information about employees or contractors? No

5) What legal authority authorizes the purchase or development of this system?
The authority for Treasury to operate the card acquiring service is codified in various statutes --31 U.S.C. §§ 321, 3301, 3302 and 3720-- which essentially provide that Treasury has authority to collect receipts and that agencies must deposit public money in Treasury and comply with Treasury regulations governing the collection of public money. The authority for Treasury to designate a financial agent provide those services is codified at 12 USC 90 and 265, which authorize Treasury to obtain banking and other services from financial institutions designated as financial agents.

DATA in the SYSTEM:

1) **Identify the category of individuals in the system**
Check all that apply:
__ Employees
__ Contractors
__ Taxpayers
_X_ Others (describe) Members of the General Public

2) **Identify the sources of information in the system**
Check all that apply:
__ Employee
_X_ Public
__ Federal agencies

__ **State and local agencies**
__ **Third party**

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

b. What information will be collected from the public?
The CAS processor Vantiv collects the minimum cardholder data (Personal Account Number, card expiration date, authorization code, etc. necessary to complete transactions regardless of the origination source (e.g., POS terminals, Pay.gov data entry, lockbox card remittance information entered in batch into Pay.gov) or type of card (e.g., magstripe or EMV chip). Cardholder name, address and other information specific to the individual (other than the PAN), are not necessary to process CAS transactions and are not collected and stored in the system as a security precaution.

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

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 (Pay.gov is an interface but not considered a "third-party" for these purposes)

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources, other than Fiscal Service records, be verified for accuracy?
Cardholder transaction number is collected at the point of sale. The authorizing bank of the card holder will check for completeness.

b. How will data be checked for completeness?
Cardholder transaction number is collected at the point of sale. The authorizing bank of the card holder will check for completeness.

c. What steps or procedures are taken to ensure the data is current?
The authorizing banks check the expiration dates of the cards and checks to see if sufficient funds are available to support the transaction during the authorization process.

d. In what document(s) are the data elements described in detail?
The ISO 8583 Financial transaction code.

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 customer initiates a sale of good from a federal agency using their credit or debit card to complete the purchase. The card number and expiration date verification allows CAS to verify that the card is valid at the point of sale allowing the issuing banks to authorize the processing of a card through the appropriate network channels.

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?
No.

4) Can the system make determinations about employees or members of the public that would not be possible without the new data?
No.

5) How will the new data be verified for relevance and accuracy?
There is no new data.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
The data is not being consolidated.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? (Explain).
Processes are not being consolidated.

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 only a list of transactions by card number. There are no other personal identity identifiers collected. There is no way to identify an individual with only the card number.

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 will not be produced on individuals. Reports are based on Transactions (amounts and PAN).

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?

If a person is trying to make an online payment to an agency (Pay.gov) and does not provide the card account number, the transaction cannot be completed.

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

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

The system currently holds records back 11 years (2006) to cover the period when the CAS Program transitioned from prior Financial Agents through to the present. The data is archived monthly, encrypted, and stored by the CAS Processor Vantiv. The program is in the process of moving to the seven (7) year retention period for financial records as specified by prevailing Bureau/RCM retention policies.

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

Automatic dispositions occur monthly (encryption/archiving) and disposition procedures are retained through the Financial Agent.

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 system is operated at two sites, where the data replication is completed within a millisecond.

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 service 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?

The Card Acquiring Service is provided by Fiscal Service's Financial Agent who employs preventative controls like annual security training for employees, and detective controls like monitoring activity on merchant records and card data.

ACCESS TO DATA:

1) **Who will have access to the data in the system?**
   Check all that apply:
   __ Contractors
   __ Users
   _X_ Managers
   _X_ System Administrators
   _X_ System Developers
   __ Others (explain)_____

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

A powerful and flexible enterprise identity management system is used that automatically manages users' access privileges within enterprise IT resources.

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

The Financial Agent is the only entity that has to the transaction data.

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)**

Detective controls are in place to monitor requests for transaction data.

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 not involved with design, development or maintenance.

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

If yes,

a. Explain the interface.

Formerly referred to as the Plastic Card Network (PCN), the Card Acquiring Service was established in 1987 (name change c. 2007) and is one of the collection mechanisms that the Fiscal Service manages for federal departments and agencies. CAS is essential to the collection of federal revenue, and processes these transactions in an efficient, timely and cost-effective manner. Federal entities, in the U.S. and abroad, rely on CAS for the acceptance of credit, debit and other payment cards (e.g., Electronic Benefits Transfer -- EBT) from customers transacting business at the point of sale, through the mail, via the internet, and over the telephone. CAS supports the major card brands (American Express, Discover, MasterCard, VISA, and regional and national debit networks).

Interfaces: Reflecting the U.S. commercial marketplace, the acceptance environment for federal agencies includes traditional stand-alone terminals, integrated point of sale (POS) systems, mobile applications, kiosks, and Internet-based software applications. The CAS acquirer/processor (Vantiv, under contract to our Financial Agent Comerica Bank) receives card transaction authorizations from these sources and via the Fiscal Service's Pay.gov internet payment portal. Pay.gov transactions also include transactions from the Fiscal Service's Revenue Collections Management (RCM) Mail channel when credit and debit card information is included on forms sent to RCM's General Lockbox Network (GLN). Funds typically settle on a next-day basis. CAS provides information to RCM's Collections Information Repository (CIR) for agency viewing and reconciliation.

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

Information Security Officers and System Owners are responsible for assuring proper use of the data. Systems management is also subject to privacy and security requirements specified in Fiscal and Financial Agent Agreements.

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.

Agencies can access their data via the CIR, a system administered by the Data Management Division of RCM, and through VantivIQ, a system provided by the CAS processor Vantiv. Users accessing data through either source are enrolled via each system.

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

Users must enroll with each system according to terms governing proper use and access controls are in in place for both CIR and VantivIQ.