

available in FMS's electronic transaction historical database or commercial databases used for verification purposes, much like a store clerk determines whether someone paying by paper check has a history of writing bad checks. The ability to research historical transaction information will help eliminate the risk of fraudulent activity, such as the purchase of government products using an account with insufficient funds or using a stolen identity. By collecting and maintaining a certain amount of unique personal information about an individual who purchases goods from the government, FMS can help ensure that the individual's sensitive financial information will not be fraudulently accessed or used by anyone other than the individual.

In addition, the information contained in the covered records will be used for collateral purposes related to the processing of financial transactions, such as collection of statistical information on operations, development of computer systems, investigation of unauthorized or fraudulent activity related to electronic transactions, and the collection of debts arising out of such activity.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

These records may be used to disclose information to:

(1) Appropriate Federal, state, local or foreign agencies responsible for investigating or prosecuting the violation of, or for enforcing or implementing, a statute, rule, regulation, order, or license, but only if the investigation, prosecution, enforcement or implementation concerns a transaction(s) or other event(s) that involved (or contemplates involvement of), in whole or part, an electronic method of collecting receipts for the Federal government. The records and information may also be disclosed to commercial database vendors to the extent necessary to obtain information pertinent to such an investigation, prosecution, enforcement or implementation.

(2) Commercial database vendors for the purposes of authenticating the identity of individuals who electronically authorize payments to the Federal government, to obtain information on such individuals' payment or check writing history, and for administrative purposes, such as resolving a question about a transaction. For purposes of this notice, the term "commercial database vendors" means vendors who maintain and disclose

information from consumer credit, check verification, and address databases.

(3) A court, magistrate, or administrative tribunal, in the course of presenting evidence, including disclosures to opposing counsel or witnesses, for the purpose of civil discovery, litigation, or settlement negotiations or in response to a subpoena, where arguably relevant to the litigation, or in connection with criminal law proceedings.

(4) A congressional office in response to an inquiry made at the request of the individual to whom the record pertains.

(5) Fiscal agents, financial agents, financial institutions, and contractors for the purpose of performing financial management services, including, but not limited to, processing payments, investigating and rectifying possible erroneous reporting information, creating and reviewing statistics to improve the quality of services provided, conducting debt collection services, or developing, testing and enhancing computer systems.

(6) Federal agencies, their agents and contractors for the purposes of facilitating the collection of receipts, determining the acceptable method of collection, the accounting of such receipts, and the implementation of programs related to the receipts being collected.

(7) Federal agencies, their agents and contractors, credit bureaus, and employers of individuals who owe delinquent debt for the purpose of garnishing wages only when the debt arises from the unauthorized use of electronic payment methods. The information will be used for the purpose of collecting such debt through offset, administrative wage garnishment, referral to private collection agencies, litigation, reporting the debt to credit bureaus, or for any other authorized debt collection purpose.

(8) Financial institutions, including banks and credit unions, and credit card companies for the purpose of collections and/or investigating the accuracy of information required to complete transactions using electronic methods and for administrative purposes, such as resolving questions about a transaction.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Debt information concerning a government claim against a debtor when the debt arises from the unauthorized use of electronic payment methods is also furnished, in accordance with 5 U.S.C. 552a(b)(12) and 31 U.S.C. 3711(e), to consumer reporting agencies, as defined by the Fair Credit Reporting

Act, 5 U.S.C. 1681(f), to encourage repayment of a delinquent debt.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:
STORAGE:

Records are maintained in electronic media.

RETRIEVABILITY:

Records are retrieved by account number (such as financial institution account number or credit card account number), name (including an authentication credential, *e.g.*, a user name), social security number, transaction identification number, or other alpha/numeric identifying information.

SAFEGUARDS:

All officials access the system of records on a need-to-know basis only, as authorized by the system manager after security background checks. Procedural and physical safeguards, such as personal accountability, audit logs, and specialized communications security, are utilized. Accountability and audit logs allow systems managers to track the actions of every user of the system. Each user has an individual password (as opposed to a group password) for which he or she is responsible. Thus, a system manager can identify access to the records by user. Access to computerized records is limited, through use of encryption, access codes, and other internal mechanisms, to those whose official duties require access. Storage facilities are secured by various means such as security guards, locked doors with key entry, and limited virtual access requiring a physical token.

RETENTION AND DISPOSAL:

Records for payments and associated transactions will be retained for seven (7) years or as otherwise required by statute or court order. Audit logs of transactions will be retained for a period of six (6) months or as otherwise required by statute or court order. Records in electronic media are electronically erased using industry-accepted techniques.

SYSTEM MANAGER(S) AND ADDRESS:

Chief Architect, Electronic Commerce, Federal Finance, Financial Management Service, 401 14th Street, SW., Washington, DC 20227.

NOTIFICATION PROCEDURE:

Inquiries under the Privacy Act of 1974, as amended, shall be addressed to the Disclosure Officer, Financial Management Service, 401 14th Street, SW., Washington, DC 20227. All