

transactions over the Internet. Another type of electronic collection mechanism known as "paper check conversion" allows the government to convert a paper check to an Automated Clearing House (ACH) debit, that is, to an electronic debit of the payor's checking account, as is done in the private sector. With better technology, FMS expects to develop new collections vehicles in the future.

FMS's electronic money programs are developed to efficiently facilitate the collection and reporting of receipts from the public in accordance with legal authorities. Simultaneously, FMS seeks to protect the government and the public from risks such as the unauthorized use of electronic payment methods, identity theft, and inadvertent disclosure of confidential information. The records covered by the proposed system are necessary not only to process financial transactions, but to authenticate the identity of someone electronically authorizing a payment to the government and to verify the payor's ability to make the payment authorized.

Thus, the records are collected and maintained for three primary reasons. First, in order to process a payment electronically, a payor needs to submit his or her name and bank account or credit card account information. Without such information, FMS would not be able to process the payment as requested by the individual authorizing the payment.

Second, to authenticate the identity of the person initiating the electronic transaction (*i.e.*, user claiming to be "John Doe" is, in fact, "John Doe"), FMS may, in some instances, require some or all of the following additional information from an individual: date of birth; driver's license number; employer's name, address and telephone number (currently, employer information is not mandatory); user name, password, and/or unique question and answer chosen by the person using the Internet to initiate the electronic transaction. The information collected and maintained for a particular transaction will depend upon the level of risk associated with the transaction. FMS will work with the Federal agency for which collections are being made to determine the financial risk associated with a transaction, as well as the risk of identity theft. For example, if an individual is paying an obligation, such as a student loan, an agency may need less information than in the case of someone purchasing goods from the government. The agency may determine there is a lower likelihood that someone would pay a bill fraudulently than there is that

someone would purchase goods in a one-time non-recurring transaction with the government. This is not to minimize the amount of security associated with an electronic loan repayment process, which in any event will be stringent, but to note that less personal information may be needed in order to provide the degree of security required for a particular transaction type. FMS recognizes that security needs must always be balanced with privacy concerns, and therefore, seeks to limit personal information requirements to only what is needed to securely process transactions.

Third, to verify the financial and other information provided by the person initiating the electronic transaction and to evaluate the payor's ability to make the payment authorized (for example, to verify the validity of the payor's credit card account information), FMS may compare information submitted with information 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.

The authentication of identity and verification of account information is required under FMS's regulation governing Federal agencies' use of the ACH system (*see* 31 CFR part 210). Part 210, which incorporates the private sector rules governing ACH transactions, requires a debit to a consumer's account to be authorized in writing and signed or similarly authenticated. For the "similarly authenticated" standard to be met, the process of obtaining a consumer's authorization electronically must provide evidence of both the consumer's identity and his or her assent to the transaction. In addition, the rules governing ACH debits initiated over the Internet require that an agency employ a "commercially reasonable fraudulent transaction detection system to screen each entry" and use "commercially reasonable procedures to verify that

(bank account) routing numbers are valid." An agency is required to retain a copy of each authorization for two years. The information collected and maintained for authentication and verification purposes is intended to assist agencies in meeting the requirements of part 210.

In addition to the purposes cited above, 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.

Thus, the information contained in the records covered by FMS's proposed system of records and FMS's use of the information is necessary to process financial transactions while protecting the government and the public from financial risks that could be associated with electronic transactions. It is noted that the proposed system covers records obtained in connection with various mechanisms that are either used currently or may be used in the future for electronic financial transactions. Not every transaction will require the collection or disclosure of all of the information listed under "Categories of records in the system." The categories of records cover the broad spectrum of information that might be connected to various types of transactions. FMS has attempted to cover the information needed for the types of transactions processed in today's technological environment, as well as some or all of the information that might be required in connection with future yet-to-be developed collections mechanisms or future security needs. Security needs are constantly changing with the evolution of technology. FMS is aware that the information used today to authenticate an individual and verify a transaction may need to be upgraded in the future.

FMS recognizes the sensitive nature of the confidential information it obtains when collecting receipts from the public and has many safeguards in place to protect the information from theft or inadvertent disclosure. When appropriate, FMS's contractual arrangements with commercial database vendors include provisions that preclude the vendors from retaining, disclosing, and using for other purposes the information provided by FMS to the vendor. In addition to various procedural and physical safeguards, access to computerized records is limited, through the use of encryption,