

Board of Governors of the Federal Reserve System, October 21, 1999.

**Robert deV. Frierson,**

*Associate Secretary of the Board.*

[FR Doc. 99-27983 Filed 10-26-99; 8:45 am]

BILLING CODE 6210-01-F

## FEDERAL RESERVE SYSTEM

### Notice of Proposals to Engage in Permissible Nonbanking Activities or to Acquire Companies that are Engaged in Permissible Nonbanking Activities

The companies listed in this notice have given notice under section 4 of the Bank Holding Company Act (12 U.S.C. 1843) (BHC Act) and Regulation Y (12 CFR Part 225), to engage *de novo*, or to acquire or control voting securities or assets of a company, including the companies listed below, that engages either directly or through a subsidiary or other company, in a nonbanking activity that is listed in § 225.28 of Regulation Y (12 CFR 225.28) or that the Board has determined by Order to be closely related to banking and permissible for bank holding companies. Unless otherwise noted, these activities will be conducted throughout the United States.

Each notice is available for inspection at the Federal Reserve Bank indicated. The notice also will be available for inspection at the offices of the Board of Governors. Interested persons may express their views in writing on the question whether the proposal complies with the standards of section 4 of the BHC Act.

Unless otherwise noted, comments regarding the applications must be received at the Reserve Bank indicated or the offices of the Board of Governors not later than November 10, 1999.

**A. Federal Reserve Bank of Boston** (Richard Walker, Community Affairs Officer) 600 Atlantic Avenue, Boston, Massachusetts 02106-2204:

1. *State Street Corporation*, Boston, Massachusetts; to engage *de novo* through its subsidiary, WFBN.com, LLC, Chicago, Illinois, in a joint venture and thereby engage in furnishing general economic information and advice and providing data processing and data transmission services, pursuant to §§ 225.28(b)(6) and (14) of Regulation Y.

**B. Federal Reserve Bank of New York** (Betsy Buttrill White, Senior Vice President) 33 Liberty Street, New York, New York 10045-0001:

1. *The Fuji Bank, Limited, Tokyo, Japan; to establish through Heller Financial, Inc., Chicago, Illinois, a joint venture between Heller's indirect, wholly owned subsidiary, Heller*

*Financial Leasing, Inc., Troy, Michigan, and SFS Holding Corporation, Park Ridge, New Jersey, an indirect, wholly owned subsidiary of Sony Corporation, Tokyo, Japan, and thereby engage de novo* through Sony Financial Services LLC in extending credit and servicing loans, pursuant to § 225.28(b)(1) of Regulation Y; and in leasing personal or real property or acting as agent, broker, or adviser in leasing such property, pursuant to § 225.28(b)(3) of Regulation Y.

Board of Governors of the Federal Reserve System, October 21, 1999.

**Robert deV. Frierson,**

*Associate Secretary of the Board.*

[FR Doc. 99-27982 Filed 10-26-99; 8:45 am]

BILLING CODE 6210-01-F

## FEDERAL TRADE COMMISSION

### Privacy Act of 1974; System of Records

**AGENCY:** Federal Trade Commission (FTC).

**ACTION:** Notice of new Privacy Act system of records.

**SUMMARY:** The FTC is establishing a new system of records subject to the Privacy Act of 1974, as amended. This system implements the requirements of the Identity Theft and Assumption Deterrence Act of 1998. The Commission will use this system to log and acknowledge complaints submitted by victims of identity theft, to provide information to such individuals, and to refer their complaints to appropriate entities.

**DATES:** Comments must be submitted by November 26, 1999. This system notice, which is being published in proposed form, shall become final and effective December 13, 1999, without further notice unless otherwise amended or repealed by the Commission on the basis of any comments received.

**ADDRESSES:** Submit comments in writing to the Office of the Secretary, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, "FTC File No. P994320, Identity Theft Program-Comment."

**FOR FURTHER INFORMATION CONTACT:** Alex Tang, Attorney, Office of the General Counsel, FTC, 600 Pennsylvania Avenue, NW, Washington, DC 20580, (202) 326-2447. For more information about the Commission's identity theft program, contact Beth Grossman, (202) 326-3019, or Joanna Crane, (202) 326-3258, Attorneys, Division of Planning & Information, Bureau of Consumer

Protection, FTC, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**SUPPLEMENTARY INFORMATION:** In accordance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a, the FTC is publishing this notice of a new agency system of records, to be designated as FTC-IV-2, "Identity Theft Complaint Management System-FTC." This system will enable the FTC to fulfill its statutory responsibilities under section 5 of the Identity Theft and Assumption Deterrence Act of 1998, Pub. L. 105-318, 112 Stat. 3007, 3010, 18 U.S.C. 1028 note ("ITADA"). The ITADA designates the FTC as a clearinghouse for the receipt and referral of identity theft complaints and requires that the FTC establish procedures: (1) To log and acknowledge receipt of complaints from individuals who certify that they have a reasonable belief that one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired in violation of the statute; (2) to provide informational materials to such individuals; and (3) to refer such complaints to "appropriate entities." Under the statute, these entities include, but are not limited to, the three major national consumer reporting agencies (currently Equifax, Experian and Trans Union), and appropriate law enforcement agencies for potential law enforcement action.

The new system of records is designed to meet these statutory requirements and will be managed and operated by the FTC's Bureau of Consumer Protection, Division of Planning & Information. The system consists primarily of a computerized database that will compile and track identity theft complaints received by the agency. Copies of identity theft complaints originally received in paper format (e.g., by mail or fax) will also be considered part of the system, but will be retained for only a temporary period after they are entered by agency personnel or contractors into the database.

Records in this system will include complaint information submitted by identity theft victims or on their behalf by others (e.g., friends or relatives). Additional sources of information will include other federal, state and local agencies ("data-contributing agencies") and retail businesses that may suspect they are dealing with an individual or entity engaged in identity theft. The FTC will use the system to log and acknowledge these complaints, to provide identity theft victims with information on how to deal with credit or other problems that may result from

identity theft, and to evaluate and refer their complaints to appropriate entities.

Until the system is fully established and operational, data from these complaints are being compiled and maintained in the Commission's general consumer complaint database (FTC-IV-1). That database, however, was not originally designed to serve the special statutory purpose for which the identity theft complaint system is being created, nor was it meant to record or track certain identity theft data that the FTC intends to collect with respect to identity theft complaints. Records in the identity theft complaint system will also be maintained and retrieved according to a somewhat broader category of individuals, as described below. Thus, the Commission is treating these complaint systems as separate systems of records for Privacy Act purposes, even if, as a practical matter, the information in both systems will reside on a common relational database and will be compiled and entered into the database by many of the same agency and contractor personnel.

Despite the sensitive nature of identity theft complaint data, the ITADA does not itself contain any provisions to protect the confidentiality of the data that the Commission is required to compile. Nonetheless, because these complaints will be collected and maintained in a system of records pertaining to individuals within the meaning of the Privacy Act, such records will be disclosed by the Commission only as authorized by that Act. See 5 U.S.C. 552a(b). The Commission intends that such disclosures will include certain necessary "routine uses" that the Commission has previously published pursuant to subsection (b)(3) of the Act, 5 U.S.C. 552a(b)(3), and made generally applicable to all of its FTC Privacy Act systems of records (e.g., use in government law enforcement litigation, where necessary). See 57 FR 45678 (1992) (Appendix I). Likewise, identity theft complaint data may also be incorporated, as appropriate, into other systems of records maintained by the Commission, such as the Commission's general complaint database (FTC-IV-1, cited earlier) or its legal investigatory files (FTC-I-1), and would be subject to any "routine uses" applicable to those systems.

The Commission has also identified certain additional "routine uses" that are necessary in order to carry out the requirements of the ITADA. These "routine uses" include referral of the complaint to a company that is the subject of the complaint or otherwise associated with the complaint, such as

the three major national consumer reporting agencies, since such entities would be in a position to resolve the complaint by taking investigative or corrective action.

Another "routine use" is disclosure of the complaint to other federal, state, or local government authorities for law enforcement or regulatory purposes. This routine use will allow referral of complaint data for investigatory purposes with or without a specific law enforcement request from such authorities, as would otherwise be required by the Privacy Act. See 5 U.S.C. 552a(b)(7). It will also allow routine disclosure of complaint records, as needed, to other regulatory agencies at the federal, state or local level so they have the information they need to identify methods or patterns of identity theft and to develop regulations, policies, or other safeguards or remedies to help stop or prevent identity theft. Once the Commission makes an authorized disclosure of complaint data to a company or another government agency, complainants should be aware that further disclosures beyond the Commission's control may not be avoidable as a practical or legal matter. The Commission intends to limit this risk by sharing complaint information only under confidentiality agreements that require that the information be used only for purposes consistent with the ITADA (e.g., resolving the individual's complaint, law enforcement or regulation, etc.).

Similarly, neither the ITADA nor the Privacy Act prevents a request for public disclosure from being filed under the Freedom of Information Act, 5 U.S.C. 552. Identity theft complaint data would normally be exempt from disclosure under that statute, however, where such disclosure would constitute a clearly unwarranted invasion of personal privacy, 5 U.S.C. 552(b)(6), or for other reasons. See, e.g., 5 U.S.C. 552(b)(7)(A) (investigatory materials that are compiled for law enforcement purposes and, if disclosed, could reasonably be expected to interfere with law enforcement proceedings).

Because the categories of individuals covered by the system may include, among others, the target of an identity theft complaint, the Commission has determined that it is necessary to exempt the system from disclosure to such individuals for law enforcement purposes, even in cases where the Commission may choose to make the complaint file available for review by the complainant or other individual who submitted the information. Thus, the Commission proposes to exempt this system of records under 5 U.S.C.

552a(k)(2), and is proposing elsewhere in the **Federal Register** to amend its Privacy Act rules, 16 CFR 4.13, to include this system in its list of systems covered by that exemption. See 16 CFR 4.13(m).

Accordingly, as set forth below, the Commission proposes a new system of records to become effective on the date noted earlier, unless the Commission amends or revokes the system on the basis of any comments received. Pursuant to 5 U.S.C. 552a(r), the Commission is providing notice of this proposal to the appropriate committees of the House of Representatives and the Senate, and to the Office of Management and Budget.

#### FTC-IV-2

##### SYSTEM NAME:

Identity Theft Complaint Management System-FTC.

##### SECURITY CLASSIFICATION:

Not applicable.

##### SYSTEM/LOCATION:

Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Records will be compiled and centrally maintained at this location, including any identity theft complaints that may be initially received or collected by the agency's Regional Offices.

##### CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

a. Individuals who communicate with the Commission to complain about or to request assistance in resolving problems relating to identity theft, or to request information concerning identity theft.

b. Individuals who submit their complaints about identity theft to another organization that has agreed to provide its consumer complaint information on identity theft to the Commission (a "data-contributing member").

c. Individuals who communicate to the Commission on behalf of another person who is the victim of identity theft. In such a case, both individuals will be covered.

d. Individuals who are suspected of committing the complained-about identity theft.

e. Individuals who, at the time the records are added to the system, are Commission employees or contractors assigned to process or respond to correspondence or telephone calls.

##### CATEGORIES OF RECORDS IN THE SYSTEM:

a. Personal identifying information about the individual who communicates with the Commission or data

contributing agency as a victim of identity theft, including, for example, the individual's name, address, telephone number, fax number, date of birth, social security or credit card numbers, e-mail address and other personal information extracted or summarized from the individual's complaint. Personal identifying information about the individual who communicates with the Commission or data-contributing agency as a reporting individual on behalf of someone else who was the victim of the identity theft, including, for example, the reporting individual's name, address, phone or fax number and e-mail address.

b. Name, address, telephone number or other information about an individual suspected of having committed the complained-about identity theft.

c. Name, address, telephone number or other information about a company that is suspected of having committed identity theft, is the subject of a complaint about how it handled the alleged incident of identity theft, or is associated with the complaint either as a creditor, debt collector, account issuer, credit bureau, or in another role (hereinafter, "company complained about or otherwise associated with the complaint"). This company information, although included in the system, is not subject to the Privacy Act.

d. Name and reference number of FTC staff member or contractor who entered or updated the complaint information in the Identity Theft Complaint Management System.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*; section 5 of the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. 1028 note.

**PURPOSE(S):**

To maintain records of complaints and inquiries concerning identity theft, in order to: enable the Commission to track and respond to complaints and inquiries; enable the Commission to refer complaints to appropriate entities, which may include referral to the three major national consumer reporting agencies and appropriate law enforcement agencies for potential law enforcement action; provide useful information that may lead to or be incorporated into law enforcement investigations and litigation or for other law enforcement purposes (when used in connection with law enforcement activities, also becomes part of FTC-I-1, Investigational, Legal and Public Records); provide useful information that may contribute to regulation and

oversight of institutions and systems that play a role in or are affected by identity theft; and provide statistical data on the number and types of complaints and inquiries about identity theft received by the agency or its data-contributing members.

**ROUTINE USES OF RECORDS, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

Records from this system may be disclosed as permitted by 5 U.S.C. 552a(b), and, as authorized by 5 U.S.C. 552a(b)(3), in accordance with the routine uses announced by the Commission in Appendix I of its system notice applicable to all other agency Privacy Act systems of records (57 FR 45678). Additional routine uses for records in this system are as follows, provided that no routine use specified either herein or in Appendix I shall be construed to limit or waive any other routine use published for this system:

a. Records may be made available or referred on an automatic or other basis to a company complained about or otherwise associated with the complaint, which may include the three major national consumer reporting agencies.

b. Records may be made available or referred on an automatic or other basis to other federal, state, or local government authorities for regulatory or law enforcement purposes.

c. Records may be incorporated, as appropriate, into other systems of records maintained by the Commission, including the Commission's consumer complaint database (FTC-IV-1) or its legal investigatory files (FTC-I-1), and subject to the routine uses published for those systems.

**DISCLOSURE TO CONSUMER REPORTING AGENCIES:**

Identity theft complaints maintained in this system of records may be referred to consumer reporting agencies (and other appropriate entities) in accordance with the Identity Theft and Assumption Deterrence Act.

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

**STORAGE:**

Stored in a computer data base maintained on magnetic disks and tape. Paper records stored in file folders.

**RETRIEVABILITY:**

Indexed by name, area code, phone number, address, state, zip code, social security number and date of birth of consumers who are the victims of identity theft. Also indexed by the name, area code, phone number,

address, state, and zip code of individuals, if any, who are identity theft suspects. Also indexed by FTC reference number, by name, address, and telephone number of company complained about or otherwise associated with the complaint, by name of other government entity or consumer reporting agency, if any, contacted by consumer in effort to resolve complaint, by name of FTC office or data-contributing agency receiving complaint, by name of Commission staff member or contractor who entered or updated the information concerning the complaint in the system database, and by other categories of retrieval.

**SAFEGUARDS:**

Paper records of incoming complaints maintained in lockable rooms and cabinets; access to computerized records by electronic security precautions, including "user ID" and password combinations and encrypted communications with external law enforcement agencies. Access restricted to those agency personnel and contractors whose responsibilities require access, or to approved staff members of external law enforcement agencies who have entered into a confidentiality agreement with the Commission.

**RETENTION AND DISPOSAL:**

Letters retained for a minimum of one year; automated information retained indefinitely.

**SYSTEM MANAGERS AND ADDRESS:**

Identity Theft Program Manager, Division of Planning & Information, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**NOTIFICATION PROCEDURE:**

16 CFR 4.13. Not applicable to the extent the system is exempt under 5 U.S.C. 552a(k)(2), as discussed below.

**RECORD ACCESS PROCEDURES:**

16 CFR 4.13. Not applicable to the extent the system is exempt under 5 U.S.C. 552a(k)(2), as discussed below.

**CONTESTING RECORD PROCEDURES:**

16 CFR 4.13. Not applicable to the extent the system is exempt under 5 U.S.C. 552a(k)(2), as discussed below.

**RECORD SOURCE CATEGORIES:**

Individuals who have complained about identity theft and others who may submit complaints on behalf of such individuals; data-contributing agencies; companies complained about or otherwise associated with a complaint.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

5 U.S.C. 552a(k)(2). See 16 CFR 4.13(m). This exemption protects records compiled for law enforcement purposes and is intended to prevent unauthorized disclosure to a target of the complaint. The Commission reserves the right to afford, at its discretion, any individual with notification, access, and contesting procedures under the Commission's rules (16 CFR 4.13) with regard to information entered or otherwise submitted by that individual into the system.

By direction of the Commission.

**Donald S. Clark,**

Secretary.

[FR Doc 99-28007 Filed 10-25-99; 10:38 am]

BILLING CODE 6750-01-P

## GENERAL SERVICES ADMINISTRATION

### Notice of Intent to Prepare an EIS; MA

The General Services Administration (GSA) intends to prepare an Environmental Impact Statement (EIS) on the following project:

#### New Federal Courthouse, Springfield, Hampden County, Massachusetts

The GSA will serve as lead agency and project sponsor in the preparation and filing of an EIS. The proposed action would involve the construction and operation of a new courthouse in Springfield, Massachusetts. Space and security constraints in the existing Federal Court facilities located in the Federal Building at 1550 Main Street, Springfield have caused the Court to seek relocation to a new building that would supply the required space, security, and facilities to accommodate the Court's current and projected caseload. This action is intended to provide approximately 140,000 occupiable square feet (13,000 square meters) of space for the various operations of the Federal Court and related agencies.

The EIS will evaluate a No-Action alternative and a Build alternative involving a preferred site on State Street between Elliot Street and Spring Street in Springfield, Massachusetts. It will also evaluate impacts on the affected environment, including, but not limited to, socioeconomics, hazardous materials, traffic/transportation, land use, urban design/neighborhood character, historic/cultural resources, noise, air quality, environmental justice, and cumulative impacts.

### Public Scoping Meeting

To ensure that all issues relating to the proposed project are identified and all potentially significant issues are addressed and satisfied in the EIS, public comments and suggestions are being solicited. To facilitate the receipt of comments, two public Scoping Meetings will be held in Springfield on Monday, November 15, 1999. The first will be held from 3 PM to 5 PM on the fifth floor of the Federal Building, 1550 Main Street, and the second will be from 6 PM to 8 PM on the second floor of the City Hall, 36 Court Street. Public comment concerning the scope of the EIS will be taken at these meetings.

#### FOR FURTHER INFORMATION CONTACT:

Kevin J. Richards, Asset Manager, U.S. General Service Administration, Portfolio Management Division (1 PT), 10 Causeway Street, 9th Floor, Boston, MA 02222-1077, Tel: (617) 565-5845, Fax: (617) 565-8650, E-mail: Kevin.Richards@gsa.gov.

Written comments may be mailed to the informational contact person no later than December 3, 1999.

Issued in Boston, Massachusetts on October 20, 1999.

#### George Klueber,

Portfolio Manager, General Service Administration, Region 1.

[FR Doc. 99-28093 Filed 10-26-99; 8:45 am]

BILLING CODE 6820-01-M

## GENERAL SERVICES ADMINISTRATION

### [GSA Bulletin FPMR H-78]

#### Utilization and Disposal

**AGENCY:** Office of Governmentwide Policy, GSA.

**ACTION:** Notice of bulletin.

**SUMMARY:** The attached bulletin provides revised information for Federal agencies on the disposal of excess biomedical equipment and IT equipment with potential Y2K defects.

#### FOR FURTHER INFORMATION CONTACT:

Martha Caswell, Personal Property Management Policy Division, Office of Governmentwide Policy, General Services Administration, Washington, DC 20405; telephone (202) 501-3846; e-mail martha.caswell@gsa.gov.

#### GSA Bulletin FPMR H-78 Utilization and Proposal

**TO:** Heads of Federal agencies  
**SUBJECT:** Disposal of Year 2000 (Y2K) Noncompliant Biomedical Equipment and Information Technology (IT) Equipment

1. *What is the purpose of this bulletin?* To provide revised information for Federal agencies on the disposal of excess biomedical and IT equipment with potential Y2K defects.

2. *When does this bulletin expire?* This bulletin contains information of a continuing nature and will remain in effect until canceled or revised.

3. *What is the background?* The Y2K technology problem concerns computers, computer chips, and software that may not properly recognize or process dates after December 31, 1999. In addition, there are other specific dates that may be troublesome, such as February 29, 2000. This problem may affect the normal operation of biomedical equipment and information technology (IT) equipment. In biomedical equipment used in direct patient treatment, the monitoring of vital patient parameters, or used to support or sustain life, the Y2K problem may present a potential risk to public health and safety if not corrected. In those situations, biomedical device failure could injure the patient or compromise effective patient treatment. In response to this potential risk, GSA is providing guidance to Federal agencies on the disposal of such equipment when it becomes excess to their needs.

4. *What does this bulletin cover?* This bulletin applies to (1) all excess biomedical equipment, and (2) all excess IT equipment.

5. *Biomedical equipment.* a. *Where can I find information about the Y2K status and potential risks posed by biomedical equipment?* Federal agencies should consult the Food and Drug Administration's (FDA's) website at <http://www.fda.gov> for general Y2K information on biomedical equipment. Federal agencies can find more specific information provided by manufacturers of biomedical equipment in the Federal Y2K Biomedical Equipment Clearinghouse (Y2K Clearinghouse) located at <http://www.fda.gov/cdrh/yr2000/year2000/html>. Federal agencies can also access the Y2K Clearinghouse through the FDA website's Year 2000 link.

b. *How can I determine the Y2K status of the biomedical equipment?* Information provided by the original manufacturer is the best source for determining the Y2K status of the biomedical equipment under consideration.

c. *Where can I find manufacturer information?* Please consult the FDA Y2K Clearinghouse website or contact the manufacturer directly.

d. *How do I use Y2K information when disposing of excess biomedical*