

(3) System NCUA-20, entitled, “Office of Inspector General (OIG) Investigative Records,” consists of OIG records of closed and pending investigations of individuals alleged to have been involved in criminal violations. The records in this system are exempted pursuant to Sections (k)(2) of the Privacy Act, 5 U.S.C. 552a(k)(2), from sections (c)(3); (d); (e)(1); (e)(4)(G); (e)(4)(H); (e)(4)(I); and (f). The records in this system are also exempted pursuant to Section (j)(2) of the Privacy Act, 5 U.S.C. 552a(j)(2), from sections (c)(3); (c)(4); (d); (e)(1); (e)(2); (e)(3); and (g).

(c) For purposes of this section, a “confidential source” means a source who furnished information to the Government under an express promise that the identity of the source would remain confidential, or, prior to September 27, 1976, under an implied promise that the identity of the source would be held in confidence.

[54 FR 18476, May 1, 1989, as amended at 60 FR 31912, June 19, 1995]

§ 792.35 Security of systems of records.

(a) Each system manager, with the approval of the head of that Office, shall establish administrative and physical controls to insure the protection of a system of records from unauthorized access or disclosure and from physical damage or destruction. The controls instituted shall be proportional to the degree of sensitivity of the records, but at a minimum must insure: that records are enclosed in a manner to protect them from public view; that the area in which the records are stored is supervised during all business hours to prevent unauthorized personnel from entering the area or obtaining access to the records; and that the records are inaccessible during nonbusiness hours.

(b) Each system manager, with the approval of the head of that Office, shall adopt access restriction to insure that only those individuals within the agency who have a need to have access to the records for the performance of duty have access. Procedures shall also be adopted to prevent accidental access to or dissemination of records.

§ 792.36 Use and collection of Social Security numbers.

The head of each NCUA Office shall take such measures as are necessary to ensure that employees authorized to collect information from individuals are advised that individuals may not be required without statutory or regulatory authorization to furnish Social Security numbers, and that individuals who are requested to provide Social Security numbers voluntarily must be advised that furnishing the number is not required and that no penalty or denial of benefits will flow from the refusal to provide it.

§ 792.37 Training and employee standards of conduct with regard to privacy.

(a) The Director of the Office of Administration, with advice from the General Counsel, shall be responsible for training NCUA employees in the obligations imposed by the Privacy Act and this subpart.

(b) The head of each NCUA Office shall be responsible for assuring that employees subject to that person’s supervision are advised of the provisions of the Privacy Act, including the criminal penalties and civil liabilities provided therein, and that such employees are made aware of their responsibilities to protect the security of personal information, to assure its accuracy, relevance, timeliness, and completeness, to avoid unauthorized disclosure either orally or in writing, and to insure that no information system concerning individuals, no matter how small or specialized, is maintained without public notice.

(c) With respect to each system of records maintained by NCUA, Agency employees shall:

(1) Collect no information of a personal nature from individuals unless authorized to collect it to achieve a function or carry out an NCUA responsibility;

(2) Collect from individuals only that information which is necessary to NCUA functions or responsibilities;

(3) Collect information, wherever possible, directly from the individual to whom it relates;

(4) Inform individuals from whom information is collected of the authority

for collection, the purposes thereof, the routine uses that will be made of the information, and the effects, both legal and practical of not furnishing the information;

(5) Not collect, maintain, use, or disseminate information concerning an individual's religious or political beliefs or activities or his membership in associations or organizations, unless:

(i) The individual has volunteered such information for his own benefit;

(ii) The information is expressly authorized by statute to be collected, maintained, used, or disseminated; or

(iii) Activities involved are pertinent to and within the scope of an authorized investigation or adjudication.

(6) Advise their supervisors of the existence or contemplated development of any record system which retrieves information about individuals by individual identifier.

(7) Maintain an accounting, in the prescribed form, of all dissemination of personal information outside NCUA, whether made orally or in writing;

(8) Disseminate no information concerning individuals outside NCUA except when authorized by 5 U.S.C. 552a or pursuant to a routine use as set forth in the "routine use" section of the "Notice of Systems of Records" published in the FEDERAL REGISTER.

(9) Maintain and process information concerning individuals with care in order to ensure that no inadvertent disclosure of the information is made either within or outside NCUA; and

(10) Call to the attention of the proper NCUA authorities any information in a system maintained by NCUA which is not authorized to be maintained under the provisions of the Privacy Act, including information on First Amendment activities, information that is inaccurate, irrelevant or so incomplete as to risk unfairness to the individuals concerned.

(c) Heads of offices within NCUA shall, at least annually, review the record systems subject to their supervision to ensure compliance with the provisions of the Privacy Act.

[54 FR 18476, May 1, 1989, as amended at 59 FR 36042, July 15, 1994]

Subpart C—Production of Nonpublic Records and Testimony of NCUA Employees in Legal Proceedings

SOURCE: 62 FR 56054, Oct. 29, 1997, unless otherwise noted.

§792.40 What does this subpart prohibit?

This subpart prohibits the release of nonpublic records or the appearance of an NCUA employee to testify in legal proceedings except as provided in this subpart. Any person possessing nonpublic records may release them or permit their disclosure only as provided in this subpart.

(a) *Duty of NCUA employees.* (1) If an NCUA employee is served with a subpoena requiring him or her to appear as a witness or produce records, the employee must promptly notify the Office of General Counsel. The General Counsel has the authority to instruct NCUA employees to refuse appearing as a witness or to withhold nonpublic records. The General Counsel may let an NCUA employee provide testimony, including expert or opinion testimony, if the General Counsel determines that the need for the testimony clearly outweighs contrary considerations.

(2) If a court or other appropriate authority orders or demands expert or opinion testimony or testimony beyond authorized subjects contrary to the General Counsel's instructions, an NCUA employee must immediately notify the General Counsel of the order and respectfully decline to comply. An NCUA employee must decline to answer questions on the grounds that this subpart forbids such disclosure and should produce a copy of this subpart, request an opportunity to consult with the Office of General Counsel, and explain that providing such testimony without approval may expose him or her to disciplinary or other adverse action.

(b) *Duty of persons who are not NCUA employees.* (1) If you are not an NCUA employee but have custody of nonpublic records and are served with a subpoena requiring you to appear as a witness or produce records, you must promptly notify the NCUA about the subpoena. Also, you must notify the