

SYSTEM NAME AND NUMBER:

SEC-21: Fitness Center Membership, Payment, and Fitness Records SEC Employee's Health and Fitness Program Records.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Securities and Exchange Commission, 100 F Street NE, Washington, DC 20549.

Areobodies Inc. 950 N Washington St Ste 313, Alexandria, VA 22314-1534.

SYSTEM MANAGER(S):

Associate Executive Director, Office of Human Resources, Securities and Exchange Commission, 100 F St NE, Washington DC 20549.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 7901, et seq.

PURPOSE(S) OF THE SYSTEM:

The system enables SEC Fitness Center staff to track Fitness Center membership, fee payments, and the physical fitness of members. The primary use of these records is to allow the SEC to provide a variety of health and fitness resources to its employees.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

SEC employees who voluntarily sign up for membership benefits for SEC fitness programs.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may contain employee name, division, office address, email address, home address, home and cell telephone numbers, date of birth, health pre-screening questions, membership number, fee and payment information (including electronic debit information), and fitness

progress charts.

RECORD SOURCE CATEGORIES:

All information is provided by Fitness Center members.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the Commission as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

1. To appropriate agencies, entities, and persons when (1) the SEC suspects or has confirmed that there has been a breach of the system of records; (2) the SEC has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the SEC (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the SEC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
2. To produce summary descriptive statistics and analytical studies, as a data source for management information, in support of the function for which the records are collected and maintained or for related personnel management functions or manpower studies; may also be used to respond to general requests for statistical information (without personal identification of individuals) under the Freedom of Information Act.
3. To interns, grantees, experts, contractors, and others who have been engaged by the Commission to assist in the performance of a service related to this system of records and who need access to the records for the purpose of assisting the Commission in the efficient

administration of its programs, including by performing clerical, stenographic, or data analysis functions, or by reproduction of records by electronic or other means. Recipients of these records shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.

4. To a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

5. To members of Congress, the Government Accountability Office, or others charged with monitoring the work of the Commission or conducting records management inspections.

6. To a commercial contractor in connection with benefit programs administered by the contractor on the Commission's behalf, including, but not limited to, supplemental health, dental, disability, life and other benefit programs.

7. To another Federal agency or Federal entity, when the SEC determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic and paper format. Electronic records are stored in computerized databases, magnetic disc, tape and/or digital media. Paper records and records on computer disc are stored in locked file rooms and/or file cabinets.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by the individual's name or membership number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with records schedules of the United States Securities and Exchange Commission and as approved by the National Archives and Records Administration.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to SEC facilities, data centers, and information or information systems is limited to authorized personnel with official duties requiring access. SEC facilities are equipped with security cameras and 24-hour security guard service. The records are kept in limited access areas during duty hours and in locked file cabinets and/or locked offices or file rooms at all other times. Computerized records are safeguarded in a secured environment. Security protocols meet the promulgating guidance as established by the National Institute of Standards and Technology (NIST) Security Standards from Access Control to Data Encryption and Security Assessment & Authorization (SA&A).

Records are maintained in a secure, password-protected electronic system that will utilize commensurate safeguards that may include: firewalls, intrusion detection and prevention systems, and role-based access controls. Additional safeguards will vary by program. All records are protected from unauthorized access through appropriate administrative, operational, and technical safeguards. These safeguards include: restricting access to authorized personnel who have a "need to know"; using locks; and password protection

identification features. Contractors and other recipients providing services to the Commission shall be required to maintain equivalent safeguards.

RECORD ACCESS PROCEDURES:

Persons wishing to obtain information on the procedures for gaining access to or contesting the contents of these records may contact the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-2376.

CONTESTING RECORD PROCEDURES:

See Record access procedures above.

NOTIFICATION PROCEDURES:

All requests to determine whether this system of records contains a record pertaining to the requesting individual may be directed to the FOIA/PA Officer, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-51002376.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

This SORN was last published in full in the Federal Register at 64 FR 19840 (April 22, 1999). Subsequent notices of revision can be found at the following citations:

- 77 FR 16569 (March 21, 2012)