SYSTEM NAME AND NUMBER: BGFRS/OIG-1, "FRB—OIG Investigative Records"

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Office of Inspector General (OIG) for the Board of Governors of the Federal Reserve System (Board) and the Consumer Financial Protection Bureau (CFPB), 1850 I Street NW, Washington, DC 20006; Axon Enterprise, Inc. 17800 N 85th Street, Scottsdale, AZ 85255.

SYSTEM MANAGER(S): Stephen Carroll, Associate Inspector General for Investigations, (202) 973-5018 or stephen.a.carroll@frb.gov; Office of Inspector General (OIG), Board of Governors of the Federal Reserve System and Consumer Financial Protection Bureau, 1850 I Street NW**,** Washington, DC 20006.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Sections 4 and 6 of the Inspector General Act of 1978 (5 U.S.C. §§ 404 and 406) and Executive Order 14074.

PURPOSE(S) OF THE SYSTEM: These records are collected and maintained by the OIG in its inquiries, investigations, and reports relating to the administration of the Board's and the CFPB's programs and operations and to manage its investigations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Officers or employees of the Board, the CFPB, or other persons related to an investigation by the OIG in order to determine whether such officers, employees, or other persons have been or are engaging in civil, criminal, or administrative wrongdoing or have information regarding such wrongdoing, relating to the Board's or the CFPB's programs or operations, and complainants and witnesses when necessary for future retrieval.

CATEGORIES OF RECORDS IN THE SYSTEM: Investigative case files, including investigative reports and related records generated or gathered during the course of or subsequent

to an investigation; electronic and hard-copy case-tracking systems; databases and applications containing investigatory information, including "Hotline" information and investigator work-papers; video and audio recordings, and other information of a personal nature provided or obtained in connection with an investigation; and memoranda and letter referrals to management or others.

RECORD SOURCE CATEGORIES: Information is provided by the individual to whom the record pertains; employees or contractors of the Board, the CFPB, and the Federal Reserve System; other government employees; witnesses and informants; and nongovernmental sources.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: General routine uses A, B, C, D, E, F, G, I, and J apply to this system. These general routine uses are located at https://www.federalreserve.gov/files/SORN-page-general-routine-uses-of-board-systems-of-records.pdf and are published in the Federal Register at 83 FR 43872 at 43873-74 (August 28, 2018). Records may also be used to disclose:

1. information to other federal entities, such as other federal OIGs or the U.S. Government Accountability Office; or to members of the Council of Inspectors General on Integrity and Efficiency (CIGIE), officials and administrative staff authorized by CIGIE to conduct or participate in assessment reviews or to a private party with which the OIG, the Board, or the CFPB has contracted for the purpose of auditing, reviewing, or conducting qualitative assessment reviews of the performance or internal safeguards and management of the OIG's investigatory program, provided that the entity acknowledges in writing that it is required to maintain Privacy Act safeguards for the information;

2. information to any source, including a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, but only to the extent necessary for the OIG to obtain information relevant to an OIG investigation; and
3. information to a federal, state, or local agency maintaining civil, criminal, or other relevant investigative information for purposes of data collection on OIG law enforcement activities.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Paper records in this system are stored in file folders with access limited to staff with a need to know. Electronic records are stored on secure servers or FedRAMP-certified cloud based systems.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records can be retrieved by numerous identifiers, including the name of the individual under investigation, the criminal investigator, the investigation number, the referral number, or the investigative subject matter.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Files related to significant investigations are cut off when the investigation is closed and permanently retained. Files related to all other investigations are cut off when the investigation is closed and destroyed ten years after cut-off.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Paper records are secured by lock and key and electronic files are stored on secure servers or FedRAMP-certified cloud based systems. The system has the ability to track individual user actions within the system. The audit and accountability controls are based on NIST and Board standards which, in turn, are based on applicable laws and regulations. The controls assist in detecting security

violations and performance or other issues in the system. Access to the system is restricted to authorized users within the Board who require access for official business purposes. Users are classified into different roles and common access and usage rights are established for each role. User roles are used to delineate between the different types of access requirements such that users are restricted to data that is required in the performance of their duties. Periodic assessments and reviews are conducted to determine whether users still require access, have the appropriate role, and whether there have been any unauthorized changes.

RECORD ACCESS PROCEDURES: The Privacy Act allows individuals the right to access records maintained about them in a Board system of records. Your request for access must: (1) contain a statement that the request is made pursuant to the Privacy Act of 1974; (2) provide either the name of the Board system of records expected to contain the record requested or a concise description of the system of records; (3) provide the information necessary to verify your identity; and (4) provide any other information that may assist in the rapid identification of the record you seek.

Current or former Board or CFPB employees may make a request for access by contacting the Board office that maintains the record. The Board handles all Privacy Act requests as both a Privacy Act request and as a Freedom of Information Act request. The Board does not charge fees to a requestor seeking to access or amend his/her Privacy Act records.

Current or former Board or CFPB employees making a Privacy Act request for records maintained by the Office of Inspector General may submit their request to the—

Inspector General

Board of Governors of the Federal Reserve System

20th Street and Constitution Avenue NW

Washington, DC 20551

You may also submit your Privacy Act request electronically by filling out the required information at: https://foia.federalreserve.gov/.

CONTESTING RECORD PROCEDURES: The Privacy Act allows individuals to seek amendment of information that is erroneous, irrelevant, untimely, or incomplete and is maintained in a system of records that pertains to them. To request an amendment to your record, you should clearly mark the request as a "Privacy Act Amendment Request." You have the burden of proof for demonstrating the appropriateness of the requested amendment and you must provide relevant and convincing evidence in support of your request.

Your request for amendment must: (1) provide the name of the specific Board system of records containing the record you seek to amend; (2) identify the specific portion of the record you seek to amend; (3) describe the nature of and reasons for each requested amendment; (4) explain why you believe the record is not accurate, relevant, timely, or complete; and (5) unless you have already done so in a related Privacy Act request for access or amendment, provide the necessary information to verify your identity.

NOTIFICATION PROCEDURES: Same as "Access procedures" above. You may also follow this procedure in order to request an accounting of previous disclosures of records pertaining to you as provided for by 5 U.S.C. 552a(c).

EXEMPTIONS PROMULGATED FOR THE SYSTEM: This system is exempt from any part of the Privacy Act, 5 U.S.C. 552a, except 5 U.S.C. 552a(b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) pursuant to 5 U.S.C. 552a(j)(2). Additionally, certain portions of this system of records may be exempt from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(2) and (k)(5).

HISTORY: This system was previously published in the Federal Register at 73 FR 24984 at 25012 (May 6, 2008). The SORN was also amended to incorporate two new routine uses required by OMB at 83 FR 43872 (August 28, 2018).