



Privacy Impact Assessment of Official Response Collaboration Application (ORCA)

This privacy impact assessment (PIA) updates and replaces the ORCA PIA dated July 22, 2020.

For Questions or Comments, please email: privacy.comments@frb.gov

Description of the IT system:

The Official Response Collaboration Application (ORCA) is a tool managed by the Board of Governors of the Federal Reserve System's (Board) Division of Board Members that allows Board staff (employees and contractors) to track the Board's official responses to:

- Members of Congress or their staff;
- Constituents or members of the public, which are forwarded by members of Congress to the Board; and
- Public or external entities (e.g., other agencies or external organizations).

All correspondence (e.g., monetary policy questions, data and statistics research inquiries, consumer complaints) are categorized in ORCA by the appropriate division or section responsible for the Board's official response. When the Board receives a correspondence, a new ticket is created. Each ticket includes pertinent information about the correspondence, along with a copy of the correspondence. Division or section administrators then assign Board subject matter experts to prepare responses. In addition to serving as a workflow management tool and repository for correspondence, ORCA is also used to track and store the Board's responses for routine reporting requirements, such as the Board's annual report to Congress.

ORCA may use artificial intelligence (AI) to more efficiently process and organize correspondence (e.g., redact personally identifiable information (PII)¹, translate foreign languages, identify keywords). Correspondence may also be used to train and improve the capabilities of the ORCA's AI tools. Importantly, AI recommendations will be verified and corrected, as appropriate, by Board staff. For instance, AI may be used to help the Board redact PII and sensitive PII² (collectively "PII") prior to posting a document publicly (e.g., public comments), such PII may include, but is not limited to:

- Social Security and passport numbers,

¹ PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The Office of Management and Budget, Circular No. A-130, *Managing Information as a Strategic Resource* (July 28, 2016).

https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

² Sensitive PII is a subset of PII, which if lost, compromised, misused, or disclosed without authorization has the potential to cause serious harm to an individual or to the Board's missions or operations.

- Financial account numbers (e.g., bank account, credit card),
- Street Addresses,
- Email addresses,
- Phone numbers,
- Dates of birth,
- Full names,
- Driver's license numbers, and
- IP addresses.

1. The information concerning individuals that is being collected and/or maintained:

ORCA may contain, but is not limited to, the following information about individual correspondents:

- Name,
- Job title/profession,
- Division/organization,
- Telephone number (business, home, or cell),
- Alternate phone number,
- Fax number (business or home); and
- E-mail address (business or personal).

Comments and questions submitted to the Board's "Contact Us" page may contain other unsolicited PII provided voluntarily by a correspondent (e.g., social security numbers, and bank account numbers).

Analysts and administrators must follow procedures to manually redact or remove PII and sensitive PII. Staff are required to remove sensitive PII provided by correspondents, and are reminded to do so in a pop-up window prior to closing out their review.

When complete redaction or removal of PII or sensitive PII is not feasible, such correspondence is labeled "Sensitive Personally Identifiable Information." This designation restricts access to only those staff members authorized to handle sensitive PII for official business purposes.

2. Source(s) of each category of information listed in item 1:

Information about individuals are derived from or related to correspondence from members of Congress, their staff, constituents, and members of the public.

3. Purposes for which the information is collected:

Although the Board does not solicit information about individuals maintained in ORCA, the Board collects and responds to these inquiries to assist members of Congress, their staff, constituents, and members of the public. The Board retains all correspondence, including associated unredacted PII, to ensure prompt responses and to maintain a searchable archive of both active and resolved communications.

4. Who will have access to the information:

Access to ORCA is restricted to authorized Board staff who have a need to know for official business purposes. Disclosures may also be subject to the Freedom of Information Act (5 USC §552), and the Privacy Act of 1974 (5 USC §552a), as described in the System of Records Notice, BGFRS-11, *Official General Files* (see question 9 below).

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses):

Individuals may decline to provide information by limiting the PII they provide, or by not submitting correspondence to the Board. The Board does not solicit or control the submission of information from members of Congress, their staff, constituents, or members of the public. Correspondents, however, do not have an opportunity to consent to the use of AI or other particular uses of their correspondence.

6. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date:

Board staff upload incoming correspondence to ORCA as it is received from correspondents. The Board does not change the information received, other than to remove or redact sensitive PII when appropriate, or verify the accuracy of the information submitted. ORCA does not allow corrections to the original requests; however, correspondents can submit a new request to correct or adjust their original inquiry.

7. The length of time the data will be retained:

ORCA maintains original correspondence and completed tickets (i.e., a record for which a response has been provided, or for which no response is deemed necessary) indefinitely in the Board's official electronic recordkeeping system.

8. The administrative and technological procedures used to secure the information against unauthorized access:

ORCA applies applicable privacy and security controls in National Institute of Standards and Technology's (NIST) Special Publication 800-53 (Rev. 5), *Security and Privacy Controls for Information Systems and Organizations*, in accordance with the Federal Information Security Modernization Act (FISMA).

Access to ORCA is restricted to authorized Board users who require access for official business purposes. The type of information users are permitted to access is based on their job responsibilities. Periodic reviews are conducted to determine whether users still require access, have the appropriate role, and whether there have been any unauthorized changes in any information maintained in ORCA. Unauthorized user IDs are tracked and investigated, as appropriate.

9. Whether a new system of records under the Privacy Act will be created. (If the data are retrieved by name, unique number or other identifier assigned to an individual, then a Privacy Act system of records may be created):

ORCA is covered by a System of Records entitled BGFRS-11, "Official General Files." [Federal Reserve Board - System of Records Notices \(SORNs\)](#).

Reviewed:

<u>//Signed//</u>	<u>10/16/2025</u>
Charles Young Senior Agency Official for Privacy	Date

<u>//Signed//</u>	<u>10/20/2025</u>
Jeff Riedel Chief Information Officer	Date