



## **Privacy Impact Assessment of Ombuds Whistleblower Claims Tracker**

**For Questions or Comments, please email: [privacy.comments@frb.gov](mailto:privacy.comments@frb.gov)**

### **Description of the IT system:**

The Ombuds Whistleblower Claims Tracker organizes, and tracks whistleblower claims regarding financial institutions received by the Federal Reserve System (FRS). A whistleblower claim is any information regarding any banking organization the Federal Reserve supervises or any director, officer, or employee of such banking organization that may have engaged in unsafe or unsound practices, violations of law or regulation, or violations of any orders or written agreements issued by the Federal Reserve.<sup>1</sup>

Whistleblower claims and information related to claims, (e.g., names of financial institutions, submission dates of claims) are stored in the Ombuds Whistleblower Claims Tracker. The Whistleblower Claims Tracker consists of a file management system and an internal collaboration site. The file management system is a collection of folders on a secured network accessible drive that stores claims submitted by whistleblowers, as well as correspondence about their claims. The internal collaboration site stores data about the claim for easy tracking and analysis by the Ombuds Office, but it does not store the actual claim or any names or contact information related to the claim.

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

Whistleblower claims submitted by individuals may include any personally identifiable information (PII)<sup>2</sup> that individuals choose to provide. While whistleblowers are welcome to report anonymously, PII typically provided by those who choose to share may include, but is not limited to the following:

- Name
- Email Address
- Phone Number

---

<sup>1</sup> <https://www.federalreserve.gov/supervisionreg/srletters/SR2207.htm>.

<sup>2</sup> The Office of Management and Budget (OMB) defines PII as 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. OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016), available at <https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>.

- Current or Former Employer

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

Individuals may submit a whistleblower claim to the FRS at any time by postal mail, email, telephone, facsimile, or via the Board's "contact us" webpage.<sup>3</sup> These submissions are voluntary. The FRS may also receive whistleblower claim referrals from other federal financial regulators (e.g., Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC)) when an agency determines the FRS should be involved in addressing the claim.

## **3. Purposes for which the information is being collected:**

Contact information provided voluntarily by individuals submitting whistleblower claims are collected to enable the Board to follow-up with individuals about their claims.

## **4. Who will have access to the information:**

Access is provided to authorized Board employees in the Ombuds Office and the Board's Legal Division (Legal) with a need to access this information to perform their job responsibilities.

If a claim involves a financial institution that is not supervised (i.e., regulated) by the FRS, staff in the Ombuds Office will typically refer it to the appropriate federal financial regulators.<sup>4</sup>

A claim relating to a financial institution that is supervised by the FRS may be shared with select staff in the Board's Supervision and Regulation Division, Division of Consumer and Community Affairs, and/or Federal Reserve Bank staff for review. The Ombuds Office may also share PII with other federal financial regulators, but only when a whistleblower provides consent to share their PII with other federal financial regulators.

## **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):**

Whistleblower claims are wholly voluntary. All whistleblowers decide whether to provide their PII (e.g., name, email, current or former employer) or to submit their claims anonymously.

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

When a claim is submitted directly by a whistleblower, the whistleblower is solely responsible for reviewing their claim and updating the Board if any of the information provided is no longer accurate (e.g., address, employment status, name). If a claim is submitted on behalf of a whistleblower by a representative, such as an attorney, the representative is solely responsible for updating the Board if any of the information provided is no longer accurate.

---

<sup>3</sup> <https://www.federalreserve.gov/apps/ContactUs/feedback.aspx>.

<sup>4</sup> In some instances, there may be overlap in supervisory authority with another agency, so the FRS may continue to investigate the claim while also sending it to other relevant agency for review.

**7. The length of time the data will be retained and how will it be purged:**

The Board is currently working with the National Archives and Records Administration (NARA) in creating a records schedule. All Ombuds Office records will be retained indefinitely until a records schedule is finalized.

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

The Ombuds Whistleblower Claims Tracker follows applicable requirements in U.S. National Institute of Standards and Technology's ("NIST") FIPS 140-3, Security Requirements for Cryptographic Modules, for encrypting data at rest and in transit. All access attempts to Ombuds Whistleblower Claims Tracker are logged and those logs are reviewed for suspicious activity. The Board also uses a third-party authentication provider for identity and management services. Access to the Ombuds Whistleblower Claims Tracker is restricted to authorized users within the Board who require access to this information in the performance of their official duties. System administrators are required to get approval prior to accessing information in the Ombuds Whistleblower Claims Tracker. Periodic audits and reviews are conducted to determine whether users still require access, have the appropriate role, and whether any unauthorized changes were made to the information maintained in the Ombuds Whistleblower Claims Tracker.

**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):**

The Ombuds Whistleblower Claims Tracker is not a System of Records under the Privacy Act of 1974 since information is not retrieved by a name or personal identifier but searched by the name of a financial institution and/or the submission date of the claim. A System of Records Notice (SORN), therefore, is not required.

**Reviewed:**

//Signed//  
Chip Young  
Senior Agency Official for Privacy (Acting)

03/01/2024  
Date

//Signed//  
Jeff Riedel  
Chief Information Officer

03/01/2024  
Date