

EEO Database System - iComplaints

Does the CFPB use the information to benefit or make a determination about an individual? Yes.

What is the purpose? Manage and Report EEO and Civil Rights complaints and cases.

Are there controls to enforce accountability? Yes, all standard CFPB privacy protections and security controls apply.

What opportunities do I have for participation? Appropriate opportunities for notice, consent, access, and redress.



Consumer Financial
Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Act), Public Law No. 111-203, Title X (2010), established the Consumer Financial Protection Bureau (CFPB or Bureau). CFPB administers, enforces, and implements federal consumer financial protection laws, and, among other powers, has the authority to protect aggrieved persons or parties from unfair, deceptive, and abusive practices when obtaining consumer financial products or services.

CFPB is committed to a work environment that promotes fairness and equality of opportunity for employees and job applicants on the basis of merit and without regard to race, color, religion, sex (including pregnancy, sexual orientation, transgender status, gender identity or expression, gender non-conformity, or sex stereotyping of any kind), national origin, disability, age (age 40 or older), genetic information, protected Equal Employment Opportunity (EEO) activity, or any other characteristic protected by federal law or executive order (collectively, “EEO bases”). CFPB has zero tolerance for unlawful discrimination, harassment, or retaliation in the workplace.

CFPB wishes to provide a neutral and impartial forum for employees, former employees, and applicants for employment to lodge complaints of discrimination based on any one or more of the protected EEO bases. Under 29 C.F.R. § 1614.104 and the Equal Employment Opportunity Commission’s (EEOC’s) Management Directive 110 (MD-110), CFPB must provide individuals access to pre-complaint counseling and an alternative dispute resolution program, offering the parties an opportunity for an early resolution of disputes in a mutually-satisfactory fashion. If the parties fail to reach a resolution, an individual may file a formal complaint of discrimination. CFPB must investigate the complaint of discrimination under 29 C.F.R. Part 1614, MD-110, and related EEOC guidance and case law.

This Privacy Impact Assessment (PIA) addresses the EEOC automated data processing system used by the CFPB – iComplaints – to store and track complaints by employees, former employees, and applicants for employment filed pursuant to 29 C.F.R. Part 1614. Data is not collected from members of the general public. iComplaints is used by the CFPB’s Office of Civil Rights (OCR) to track EEO complaints. iComplaints is a commercial-off-the-shelf (COTS) web-based service, hosted by an off-site vendor, MicroPact Engineering, Inc. The federally mandated reports generated by the system are the Annual 462 Report and the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act) Report.

Individuals receive constructive notice from this PIA and the government-wide SORN EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records (July 30, 2002, 67 FR 49338, 49354-55). You can read the SORN here: <http://www.gpo.gov/fdsys/pkg/FR-2002-07-30/pdf/02-18895.pdf>

Privacy Risk Analysis

The primary privacy risks associated with this implementation of the EEO database system are risks related to:

- Data minimization
- Confidentiality

Data Minimization: CFPB limits the scope of information collected in iComplaints to the amount of data necessary to act upon the complaints filed. Although the system stores PII provided in the complaint, this information is captured only where it is relevant to a complaint, claim, and/or an investigation. The information included in the EEO database system contains information collected directly from the individual who is filing a complaint, or people responding to, or with knowledge of, the complaint. Because the interactions that result in information collection are generally voluntary, and because the Bureau does not use any information collected through these process to deprive an individual of a right or benefit, the privacy risks associated with these collections are minimal. Complainants choose what and how much information they share with the Bureau and they have opportunities to change or update information that is erroneous or no longer accurate or relevant. Direct identifying PII is generally limited to names and contact information (address, phone, date of birth, email, professional affiliation or employer) which is required as part of the complaint process to process a complaint.

Confidentiality: In the event of a breach of confidentiality, there is a risk of embarrassment or loss of reputation to both the individual and the Bureau. A breach of confidentiality could result in complainants suffering financial harm as a result of identity theft. The Bureau minimizes this risk by enforcing access controls to minimize the number of individuals who have access to the data and by storing data on systems that have been accredited as secure for this type of data. Staff is also trained on how to handle potential breaches to minimize negative impacts.

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

Privacy Risk Management

1. Describe what information the CFPB collects, how the information is collected, and the sources from which the information is collected.

Personal information collected by the system includes:

- Name
- Truncated SSN
- Employee Identification Number
- Date of Birth
- Mailing Address
- Work Phone Number
- Home Address
- Home Phone Number
- Disability Information
- Employment Information
- Education Records
- Date of Request for Alternate Dispute Resolution (ADR)
- Protected Class Information (e.g., race, age, national origin, color, disability, religion, sex (including sexual orientation), genetic information)
- Other identifying information as relevant to the matter

Results of fact-based inquiries (e.g., direct, comparative, and statistical evidence and information such as forms, sworn and/or unsworn statements of fact, reports and summaries) created and collected by counselors, investigators and EEO professionals responsible for the administrative processing of the allegations of discrimination are also input into the database. Over 500 data fields are captured in iComplaints giving CFPB the ability to identify the issues and basis of the complaints, the complainants, the witnesses, and other information necessary to analyze complaint activity and trends, but also the ability to track and monitor the location, status, and length of time elapsed at each stage of the complaint resolution process consistent with EEOC Management Directive (MD)-110. Although certain information is mandatory, most of the information collected is captured only where it is material and relevant to a complaint, claim, and/or an investigation.

Information pertaining to the claims and issues raised within the complaint is collected primarily from persons filing complaints, co-workers, supervisors, witnesses and legal representatives with knowledge of the allegations. Because individuals who are not CFPB employees may file a complaint, information about non-CFPB employees may also be collected.

2. Describe CFPB's objective for the information.

The information is collected for the administration, processing, and resolution of complaints. It is a requirement that the iComplaints system be able to accurately identify the individual who is making the complaint, and that the information to contact the complainant is accurate and up to date.

iComplaints may also aggregate data (through basic and ad hoc search functions) in order to show trends (e.g., division data, fiscal year data, and case status data). Trend analyses require a statistically significant pool of archival data over the course of several years to properly assess the EEO climate and the effectiveness of process improvement and/or pilot programs. CFPB uses all of this information to determine the status of compliance with EEOC MD-110 and the EEOC Management Directive 715 standards for model EEO program status.

The data stored in iComplaints may also be used by the Bureau for reporting and statistical purposes with personal identifiers removed.

The CFPB may share the information contained in the complaint with a staff or third-party counselor, mediator or other neutral during either the informal or formal phases of the complaint process. The information provided will assist the neutral in conducting counseling or mediation, in order to attempt to resolve the complaint.

If the complaint is not resolved informally (through ADR or otherwise) and the complaint meets the criteria for acceptance, the CFPB will conduct an investigation of the complaint, either with its staff or through the use of qualified third-party investigators, which will include a thorough review of the circumstances under which the alleged discrimination in employment occurred, along with evidence from which the ultimate factfinder is able to determine whether or not any violation of EEO laws has occurred. Investigators must be (and must maintain the appearance of being) unbiased, thorough, and objective. By gathering the relevant information and documentation, the EEO investigator plays a critical role in helping prepare the factual record, which allows a factfinder to draw factual conclusions as to whether discrimination has occurred.

The conclusion of the EEO complaint process allows complainants an opportunity to elect a forum to have the merits of their case decided, *i.e.*, a Final Agency Decision (FAD) issued by CFPB or a hearing before an EEOC Administrative Judge. Upon election of a FAD, Office of Civil Rights (OCR) may provide a third-party vendor with a redacted report of investigation (ROI) which always excludes social security numbers and PII not needed by the vendor. Upon election of a hearing, OCR provides the EEOC a redacted report of investigation (ROI) which always excludes social security numbers and PII not needed by the vendor. The complainant, his/her representative and persons within CFPB's Legal Division also receive a copy of the ROI.

3. Describe how CFPB shares any of the information with third parties with whom the CFPB shares the information for compatible purposes, e.g. federal or state agencies, the general public, etc.

Information related to EEO complaint activity is shared with other federal and state authorities, such as the Office of Personnel Management (OPM), EEOC, Merit Systems Protection Board (MSPB), Department of Justice, and Congress. Disclosures are made in accordance with the Privacy Act and the applicable SORN, EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records (July 30, 2002, 67 FR 49338, 49354-55).

If the complainant decides later to either appeal the matter to a federal appellate court, as appropriate, or to file a complaint of discrimination in a federal district court, the information may be shared with the federal court and consequently be a matter of public record.

Aggregate EEO complaint data is also made available publically and is updated quarterly on the www.consumerfinance.gov website through No FEAR Act statistical data. The CFPB also provides comprehensive statistical EEO data to the EEOC on an annual basis. The CFPB provides an annual No FEAR Act Report containing statistical and analytical data to Congress and other federal agencies.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

iComplaints does not specifically require individuals to provide any of their personally identifying information; however, the processing of an EEO complaint is limited when contact information is not provided. The CFPB gives individuals the ability to request access and amendment to their personal information in accordance with the Privacy Act and the CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 *et seq.* Individuals may also file a request under the Freedom of Information Act. A Privacy Act notice is part of the investigation affidavit provided to all witnesses who are asked to give written testimony as part of the EEO investigation and is included in the ROI that the complainant receives. This notice ensures that the individual is aware that the collection of information will be included in an agency system of records.

5. Explain the standards and relevant controls that govern the CFPB's—or any third party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

The Bureau complies with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002; voluntarily adopts Office of Management and Budget privacy-related guidance as a best practice¹ and applies National Institute of Standards and Technology risk management processes for privacy.

The CFPB uses the following technical and administrative controls to secure the data and create accountability for the Bureau's appropriate collection, use, disclosure, and retention of the information:

- Audit Logs and Reviews

¹ Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with Office of Management and Budget (OMB)-issued privacy guidance; it follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

- CFPB Personnel Privacy Training
- CFPB Privacy Incident Response and Recovery Plan
- Compliance with CFPB cybersecurity policy and procedures
- Policy and Standard Operating Procedures
- Role-based Access Controls
- Records Schedule Submitted to/Approved by National Archives and Records Administration: General Records Schedule 1, Item 25 (Equal Employment Opportunity Records)
- Personnel Security including background checks

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the CFPB, e.g., government contractors discussed in Question 5.)

Only CFPB employees or contractors acting on behalf of the CFPB will have access to the system. No other systems share or have access to the data in iComplaints.

Document control

Approval

Ashwin Vasan

Chief Information Officer

Date: October 13, 2015

Claire Stapleton

Chief Privacy Officer

Date: October 13, 2015

Name

M. Stacey Bach

Assistant Director, Office of Civil Rights

Date: October 13, 2015

Change control

Version	Summary of material changes	Pages affected	Date of change