OCR Equal Employment Opportunity (EEO) Program

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Administration of EEO Program.
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.

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law No. 111-203, Title X (Dodd-Frank), established the Consumer Financial Protection Bureau (CFPB) and through which it administers, enforces, and implements federal consumer financial protection laws. As a federal government employer under the Equal Employment Opportunity Act, Public Law 92–261, CFPB is required to provide a work environment that is free from discrimination and harassment. It is the policy of CFPB to provide equal employment opportunity to all employees and applicants for employment. CFPB has no tolerance for workplace discrimination, harassment, or retaliation, and takes all allegations of discrimination, harassment, and retaliation seriously.

To fulfill this mission and ensure a work environment that promotes fairness and equality, CFPB created the Office of Civil Rights (OCR) – CFPB's Equal Employment Opportunity (EEO) Program. OCR is an independent, impartial, and confidential resource that evaluates, and when appropriate, investigates and adjudicates the claims CFPB employees, former employees, or job applicants who believe they were discriminated against or harassed on the bases of 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 (40 years or older), genetic information, parental status or retaliated against for prior EEO activity. OCR collects, uses, maintains, and shares personally identifiable information (PII) to perform EEO activities, including first name, last name, email address, and details specific to complaints involving CFPB employees, employee ID number, division and office assignment, occupational series, grade, and position title.

A major part of OCR's work is receiving and processing claims of discrimination, which are directly communicated to OCR by employees, former employees, and applicants. Various laws, regulations, and Office of Inspector General (OIG) findings require CFPB to securely capture specific data, including PII, about claims of EEO discrimination. To ensure the accurate and secure handling of data involved in EEO cases, OCR uses a commercial off-the-shelf (COTS) product to manage case activities and a cloud-hosted secure data transfer system to manage secure communications involving PII. Both systems are hosted by third party service providers that allow OCR the ability to collect, track, manage, process, and report on information submitted to OCR related to discrimination or harassment inquiries under its purview. This includes information about individuals who inquire about submitting a complaint, those who actually submit a complaint, and those who are related to or subject to a complaint. OCR uses these systems to allow authorized CFPB staff to retrieve and send documents to and from internal and external complainants and complainant representatives. These systems also allow OCR to collect

and manage data for each EEO case. These technologies provide a clear audit trail of when authorized users take certain key actions such as opening a case or file to review it, or when a file was received or sent. These technologies employ an agile methodology for operational maintenance, where the systems are developed on an ongoing basis by the third-party vendor and CFPB staff. As a result, privacy compliance is considered and integrated into the development process and is documented in system change requests and security assessments and authorizations (SA&A) each systems.

CFPB provides individuals notice of the information collected and maintained by OCR and the uses of this information to support OCR activities through publication of this Privacy Impact Assessment (PIA) and from the Equal Employment and Opportunity Commission (EEOC)/GOVT-1 - Equal Employment Opportunity in the Federal Government Complaint and Appeal Records System of Record Notice (SORN).[1] The collection of CFPB users information to access and maintain the system is covered by CFPB.014 - Direct Registration and User Management System (DRUMS) SORN. The Paperwork Reduction Act (PRA) does not apply to the use of these technologies. The collection and use of data used within the case record is sourced directly from complainants and from individuals and third parties involved in an EEO case.

This PIA addresses the collection, use, sharing, and maintenance of PII used by the EEO Program and the impact of the systems that OCR uses to support EEO processes.

Privacy Risk Analysis

The primary privacy risks associated with this application are related to:

- Individual Participation
- Data Minimization
- Limits on Uses and Sharing of Information
- Security

Individual Participation

Under Dodd-Frank and the Equal Employment Opportunity Act, Public Law 92–261, OCR

[1] EEOC/GOVT-1 - Equal Employment Opportunity in the Federal Government Complaint and Appeal Records is a government wide SORN, applicable to all systems of records that are maintained for the purpose of counseling, investigating and adjudicating complaints of employment discrimination brought by applicants and current and former federal employees against federal employers.

collects information from complainants who may be current employees, former employees, or job applicants. OCR is authorized to receive additional information collected by the Office of Human Capital (OHC), as appropriate, about CFPB employees in support of an EEO investigation, and collect information from complainant representatives or third parties associated with an EEO case. In some cases, individuals that are part of an EEO investigation may not be aware of their involvement. To the extent possible, OCR provides notice of the collection and use of PII in support of EEO complaints leading to investigations. However, in some cases, notifying individuals of their involvement in an EEO case may compromise the investigation process. The risk of collecting information, which may include PII, from individuals not directly associated with the complaint and EEO investigation is accepted by CFPB as part of its duty to evaluate, and when appropriate, investigate and adjudicate claims. Individuals that become aware of the use of their data in an EEO case may contact CFPB to request access to amend, and remove their information as appropriate, unless doing so disrupts or compromises an active EEO investigation. If CFPB engages with individuals that are not directly involved with a complaint to collect details about the case, CFPB provides the individual appropriate notification of the reasons why their information has been collected and the uses of this information.

Data Minimization

There is a risk that more than the necessary information is collected from individuals who wish to submit a complaint. This risk is mitigated by the general practice that CFPB always collect the minimum amount of PII necessary to complete a task related to its mission. The information, including PII, is limited to what is provided directly by individuals to OCR, CFPB staff records collected as applicable to an EEO activity, and PII received in response to a complaint. OCR may also receive information from OHC. The OCR in consultation with OHC, the Privacy team, and other teams as appropriate ensures that PII is shared only on a need to know basis. Individuals may choose what and how much information they share with OCR. They also have opportunities to amend and correct records in accordance with the Privacy Act of 1974. The minimum amount of PII collected includes first name, last name, email address, and details specific to claims involving CFPB employees, employee ID number, division and office assignment, occupational series, grade, and position title.

Limits on Uses and Sharing of Information

There are risks that the information collected and maintained by OCR may be misused or used for unauthorized purposes. Given the sensitive and confidential nature of the claims and OCR's role in processing the claims, there is also a risk of embarrassment or loss of reputation to both individuals filing complaints and CFPB if EEO case information is sent to an unauthorized recipient. CFPB minimizes this risk by enforcing access controls that limit access to data to only

authorized OCR staff and individuals directly involved in an EEO case. OCR staff sign a non-disclosure agreement (NDA) and are also trained on appropriate uses of the data within the application, prior to being granted access to the application. Case records and the PII within them are only accessible to OCR staff or other designated OCR staff/offices (i.e., when a complaint is appealed and goes to the EEOC).

Security

Given the content and sensitivity of information to be held within the application, there is a risk that unauthorized individuals may gain access to the information. CFPB mitigates this risk in several ways. As a third-party system, federal standards, and regulations for safeguarding private information apply; CFPB must conform to federal security requirements and guidance, such as the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Information Systems and Organizations. Additionally, by using the cloud-hosted data transfer system, the CFPB is enhancing its method of securely communicating documentation, including documents containing PII.

Access to the data itself is also limited. Access controls, along with other security measures are in place to securely submit data to OCR and limit case file data only to OCR staff. External individuals must access a file sent by OCR using multi-factor authentication (MFA), and data provided externally is available for a defined period set by OCR and then access to the data is terminated. Access for authorized OCR staff is based on their need to know and is restricted to the minimal amount of data required or appropriate to carry out their assigned job responsibilities. The CFPB terminates or reduces access as necessary should the staff member no longer have a need to know the information, change job functions, is terminated, or resigns. Information is also subject to the appropriate technical, physical, and administrative controls implemented to address these risks, such as encryption for data maintained within the system. For example, NIST controls families, including Identification and Authentication (IA) and Risk Assessment (RA), are implemented to restrict access to the information to authorized OCR Staff.

The technical, physical, and administrative controls are implemented to limit uses of and sharing of PII, securing the application, and minimizing data to the amount necessary are appropriate for the purpose of the application.

Privacy Risk Management

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

When an individual contacts OCR to inquire into a discrimination claim (by email, phone, or mail), an authorized OCR staff person collects their information (including any related PII), creating a case file. Copies of these records and communications, along with subsequent materials that emerge during the processing of the case are stored with the case file, which is stored within the system as a digital case record. The information collected from the individuals at this point in the process may include their first name, last name, email address, employee ID number, division and office assignment, occupational series, grade, and position title. It may also include the first name and last name, email addresses, and details specific to issues of other employees that are the subject of the complaint or otherwise involved in the complaint. All information is provided voluntarily by an individual submitting the complaint, however, a minimum amount of data, including PII, must be provided to identify the issue and to contact the individual making a complaint for follow-up discussion and potential resolution.

If an individual chooses to pursue the EEO process, the case file is then assigned to an authorized OCR staff member (e.g., EEO counselor, EEO investigator, or EEO Attorney-Advisor) to manage the case. Case files can only be viewed by authorized OCR staff who have a need to know. OCR may use this information to evaluate a claim based on the applicable laws, regulations, and CFPB policies. OCR also engages the individual and/or stakeholders involved during a comprehensive investigation. During the investigation and resolution of a claim OCR staff meet with CFPB officials to discuss the issue(s) and may make the decision as to whether discrimination occurred, in violation of a civil rights law. CFPB may request additional information, including PII, regarding the complaint to support an EEO investigation. When requested, an OCR staff member can provide the complainant with a link to a secure file transfer system to submit this information.

At each stage of this process, information describing the actions taken is documented within the case file. Records provided by the complainant or that emerge during the lifecycle of the complaint, along with documentation of the case by the EEO Counselor, EEO Investigator, or EEO Attorney-Adviser are attached to case files as a system of record. During this process, identifying information is not shared by the case manager assigned unless the individual consents, or if it is determined there is an imminent risk of serious harm, the issue concerns government fraud, waste, or abuse, or if required by law. Additional employee data may also come from the Office of

Human Capital (OHC). For specific circumstances, like fulfilling mandatory reporting requirements, OHC shares PII necessary to ensure accuracy in the EEO case file.

OCR files an annual Notification and Federal Anti-Discrimination and Retaliation Act of 2002 (No FEAR Act) report and the Annual Federal Equal Employment Opportunity Statistical Report of Discrimination Complaints (EEOC Form 462). The annual No FEAR Act Report is reviewed by the CFPB Director as part of CFPB's clearance process and published on consumerfinance.gov (CFPB's public website). OCR data may be used to conduct analysis of trends as part of the barrier analysis work required by EEOC Management Directive (MD) 715. A quarterly No FEAR Act report is also produced and published on consumerfinance.gov. Other periodic reports may be produced in response to ad hoc inquiries. OCR data may also be used to identify trends and similar occurrences within the collected data that informs future decisions by CFPB related to employment discrimination and harassment. No PII of any kind is included within reports shared outside of OCR.

Given the content and sensitivity of information collected and used by OCR, strict, transparent access controls are employed based on roles and responsibilities. This ensures confidentiality and security of data used by OCR by limiting it only to authorized CFPB and technical staff.

2. Describe CFPB's objective for the information.

OCR collects PII to identify, process, and resolve discrimination complaints submitted by complainants. OCR uses PII to document complaints and collect other information as necessary while a complaint is being investigated. This includes any appeals or the transfer of cases to other CFPB offices or agencies as necessary to complete the investigation. Details from the case record are also used when engaging the individual and/or stakeholders who are relevant to the complaint, including CFPB officials, complainants, complainant representatives, and OHR. After the conclusion of this process, case files are stored for record keeping.

In each stage of the EEO process, information describing every case "event", including PII identifying individuals, are documented within the case file. The objective in using this information is to assist with the assessment of an individual's issue or complaint to a fair and reasonable resolution, to ensure compliance with regulatory timeframes for processing EEO complaints, and to analyze the aggregate data for trends. The PII collected is used for two primary purposes – case management, and system and EEO Program administration.

Case Management

OCR uses a case management information system that allows authorized OCR staff to create cases, track case logs, track regulatory timeframes, monitor emerging trends in cases, and comply with periodic reporting mandates. OCR staff creates a case file when an individual contacts OCR about a potential adverse action. To do this, the individual contacts OCR and provides in as much detail as possible, the event, issue, or information that led to equal employment opportunity concerns. The individual must include their first and last name, address, phone number, and email address to create a case. A case record is created once all this has been provided, and the case is then assigned to an OCR staff member to manage the case. If more information is required, OCR may reach out to individuals involved with the case to collect additional information, which may include PII, using a secure data transfer process. The case record may eventually include the first name and last name of other CFPB employees, email addresses, and details specific to issues involving the claims against the CFPB staff in question, employee ID numbers, division and office assignments, occupational series, grade, and position title. To collect this additional information OCR can use the secure transfer system to provide a link to a specific individual along with a request for additional information. The link allows the individual to upload relevant documentation that is then securely submitted to OCR, and attached to the case file. All the available documents associated with a complaint are then tracked as part of the case record.

The information from complainants is provided voluntarily, and is collected to assist OCR in addressing the subject complaint. OCR only uses this information in accordance with applicable laws, regulations, policy, such as to interact with the individual and/or stakeholders involved, meet with CFPB officials to discuss the issue, and to make a final determination as to whether discrimination existed in violation of a civil rights law. At each stage of this process, information describing every major case processing "event," is documented within the case record. During these processes, PII is not shared by the system nor by the case manager assigned to the case unless the subject individual consents, or if it is determined there is an imminent risk of serious harm, the issue concerns government fraud, waste, or abuse, or if required by law.

Depending on the nature or path of a potential case, it may be transferred for further deliberation or review. No access outside OCR administration is granted unless approved by OCR leadership. Federal guidelines for confidentiality and handling sensitive information dictate how case files are transferred in a secure manner. Any transfers of case information are executed using a secure data transfer system as described above.

System administration

OCR collects and uses PII for administration of EEO processes. PII of CFPB staff and authorized technical support from third-party vendors are used for access and identity management of the

systems that support the EEO process. OCR utilizes single sign on (SSO) supported by Active Directory with a roster feed of authorized OCR CFPB staff that is updated bi-weekly. Access is managed by the designated System Owner or OCR Director and in general is based on the role of individual CFPB or technical staff in relation OCR program or support they provide for the system.

Reporting

Data collected within case files is used by OCR to produce several reports associated with the Program (e.g., No FEAR Act Annual and Quarterly Reports, Form 462). CFPB also produces the Equal Employment Opportunity (OCR) Program Status Report (herein referred to as the "Report"), which is submitted under the EEOC's MD-715. MD-715 requires Federal agencies to conduct a self-assessment on at least an annual basis to evaluate the effectiveness of their overall Equal Employment Opportunity program, using EEOC-prescribed compliance indicators and measures. MD-715 also requires agencies to identify any institutional, structural, attitudinal, and/or physical barriers that may operate to exclude certain groups, and to develop action plans to eliminate identified barriers. The Report is the result of CFPB's annual self-assessment. Aggregate and narrative data informs parts of the report; no PII is published. OCR executes an internal review process for PII and other concerns, prior to their publication.

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.

OCR, in accordance with the requirements of EEOC's regulations, requires individuals to provide their PII for a complaint to be initiated, collecting only a minimum amount of necessary to conduct its duties. Within CFPB, only OCR staff and others with a need to know are granted access to the relevant PII associated with a complaint. If the case is further pursued for a hearing at the EEOC, then it is transferred using the secure data transfer system to the EEOC for the administrative judicial process, with litigation in federal district court also a possibility. In those instances, the PII of those involved in the case is shared.

An assigned OCR manager can share PII from a case record under the following circumstances: with the individual's consent; if it is determined there is an imminent risk of serious harm; the issue concerns government fraud, waste, or abuse; or if required by law (i.e., sharing the case with another federal agency) or in accordance with the routine uses published in the EEOC/GOVT-1 SORN. These records are maintained and shared for the purpose of counseling, investigating and adjudicating complaints of employment discrimination brought by applicants and current and former federal employees against federal employers.

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.

When an individual provides information to OCR, they are given notice that what they are submitting will be entered into a system for further use by OCR for the purposes of responding to a complaint. The publication of this PIA and the EEOC/GOVT-1 – Equal Employment Opportunity in the Federal Government Complaint and Appeal Records SORN provide notice of the collection of PII for OCR purposes and intended use of PII by CFPB. CFPB gives individuals the ability to request access and amend their personal information in accordance with the Privacy Act and CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq.

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.

OCR employs vendor-hosted, cloud-based business process management tools and secure data transfer systems that are compliant with federal security and privacy requirements. This includes privacy requirements associated with the Equal Employment Opportunity Act of 1972, Privacy Act of 1974, Right to Privacy Act, and E-Government Act of 2002, along with the application of recommendations of guidance from the Office of Management and Budget. Access to the data that are collected and the case file itself is limited solely to OCR staff through a secure web interface. Authorized OCR staff collect information directly from individuals who contact the Office in relation to their discrimination inquiries. OCR employs the secure data transfer system to securely send information about a case between authorized CFPB OCR staff and individuals related to the complaint. PII of CFPB staff who are involved in OCR administration or involved in the claim, is also collected, and sourced from CFPB systems.

CFPB assesses all technologies that support OCR EEO processes to ensure that PII collected, used, shared, and maintained, is protected and secure. CFPB uses the following technical and administrative controls to secure the data and create accountability for CFPB's appropriate collection, use, disclosure, and retention of the information:

- Implementation of applicable National Institute of Standards and Technology (NIST)

800-53 control(s)

- Audit Logs and Reviews
- CFPB Personnel Privacy Training
- CFPB Privacy Breach Response and Recovery Plan
- Compliance with CFPB cybersecurity policy and procedures
- Data Quality and Integrity Checks
- Policy and Standard Operating Procedures
- Role-based Access Controls[2]:
    - Master Administrator – Senior OCR staff, grants permission for user roles and access to the system; must complete CFPB training for privacy and information security
    - Administrator – Vendor staff, responsible for deployments and technical configuration; must complete CFPB privacy and information security training for contractors, no access to CFPB data
    - Case Processor – CFPB staff with access only to cases which are assigned to or created by them; must complete CFPB training for privacy and information security
    - Super Processor – Senior OCR staff with access to all cases regardless of who created it or who it is assigned to; must complete CFPB privacy and information security training
    - Domain Administrator – Technical CFPB staff, responsible for server maintenance/configurations, patching, remediation, and provisioning. They support enforcement of security controls, management of network firewalls, switches, and routers. Oversees hosting infrastructure. No access to cases files; must complete CFPB privacy and information security training
    - Middleware Team– Technical CFPB staff, responsible for managing middleware team activities, including production deployment, routine maintenance, authentication within applications. No access to cases files; must complete CFPB privacy and information security training
    - Database Administrator Team – Technical CFPB staff, responsible for database

[2] Only staff from CFPB OCR have access to case files and the PII contained in them. Technical support staff from the vendor and the CFPB are granted access to the system, only after approval and when they have a need to know.

management and security. Activities include supporting configuration of databases, backups of data, and overall data retention. No access to cases files; must complete CFPB privacy and information security training

- Records Retention requirements: CFPB maintains matters in accordance with the following National Archives and Records Administration (NARA) approved schedules:[3]
    - GRS 2.3, Item 110 (Equal Employment Opportunity (EEO) discrimination complaint case files – Informal process): DAA-GRS-2018-0002-0012
    - GRS 2.3, Item 111 (Equal Employment Opportunity (EEO) discrimination complaint case files – Formal process): DAA-GRS-2018-0002-0013

Systems used by OCR to manage EEO processes are not accessible to the public or anyone within or outside CFPB that does not have prior authorization. Authorized staff from the vendor may be granted access to the system to provide technical support.

As a result of conducting this assessment, the PIA has been updated to consider the impact of technologies that support OCR EEO processes, and ensure that those technologies are appropriately assessed for use within CFPB.

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 and contractors acting on behalf of the CFPB have access to the system, which may include authorized staff from system vendors to provide technical support. No other systems or individuals have access to the data within the OCR EEO process. OCR is required to create annual and quarterly reports detailing trends and measurements associated with the OCR program. Data from case files inform this document but reports do not contain PII. The reports utilize aggregate and de-identified data in their findings. CFPB employs a review process prior to the publication of these reports, to ensure that PII and sensitive information are not published.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2023.05.16 14:41:34 -04'00'

Chris Chilbert

Chief Information Officer

Date

Kathryn Fong

Digitally signed by Kathryn Fong
Date: 2023.05.16 16:00:37 -04'00'

Kathryn Fong

Acting Chief Privacy Officer

Date

Lori Grant, Deputy Assistant Director

Digitally signed by Lori Grant, Deputy Assistant Director
Date: 2023.05.16 14:09:41 -04'00'

Lori Grant

Deputy Director, Office of Civil Rights

Date