

# OCR Database System – Entellitrak’s ETK EEO

---

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

No.

---

**What is the purpose?**

Manage and report EEO 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, Public Law No. 111- 203, Title X (Dodd-Frank), established the Consumer Financial Protection Bureau (CFPB or Bureau) 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, the Bureau 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. The Bureau 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) – the Bureau’s Equal Employment Opportunity (EEO) Office. 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 to the Bureau, 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.

A major part of OCR’s work is receiving and processing claims of discrimination, which are directly communicated to the Office by employees or applicants. Various laws, regulations, and OIG findings require CFPB to securely capture specific data about these claims of EEO discrimination. To ensure the accurate and secure handling of these cases, OCR uses a case management system to document claims and maintain the information collected about them. The system also supports producing data that informs mandated reports about these activities.

For this function, OCR previously used the iComplaints system. As a result of the vendor sunsetting the software, the Bureau is now using Entellitrak’s “ETKEEO”, the replacement for iComplaints. This Privacy Impact Assessment (PIA) addresses the OCR instance of the Entellitrak application and replaces the EEO Database System – iComplaints PIA (published October 13, 2015).

Entellitrak is an enterprise level commercial off-the-shelf (COTS) product hosted by a third party service provider that provides OCR staff with the ability to collect, track, manage, process, and report on information submitted to OCR related to discrimination or harassment inquiries under its purview. This may include information about individuals who are inquiring into submitting a claim, those who actually submit a claim, and those who are related to or subject to a claim. Entellitrak also maintains user account information of OCR staff, Bureau technical staff, and staff from the vendor -

who maintain the Entellitrak system. The information in Entellitrak includes any personal identifiable information (PII) which is needed to fulfill its functions. Individuals submitting a complaint provide their information to OCR staff during an intake process and it is entered into the system. PII for Bureau staff is sourced from internal databases and systems.

Individuals receive notice of the information collected and maintained in this system and the uses of this information to support OCR activities in this 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).<sup>1</sup> The collection of users information to access and maintain the system is covered by CFPB.014 - Direct Registration and User Management System (DRUMS) SORN.

Entellitrak employs the agile methodology for operational maintenance, where it will be developed on an ongoing basis by the third-party vendor and Bureau staff. As a result, privacy compliance is integrated into the development process and will be documented in system change requests and security assessments and authorizations (SA&A), where accounting for privacy will be in the statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment.

The Paperwork Reduction Act (PRA) does not apply to Entellitrak. The collection and use of data used within the case record is sourced from information provided to OCR that will be used to create and track issues and complaints. Entellitrak does not ask “identical” questions of ten or more persons as defined in 5 CFR 1320.3(c).

## 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

---

<sup>1</sup> 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.

### ***Individual Participation***

As part of the intake process for creating a case file within Entellitrak, OCR staff directly collect and enter information provided by individuals interested in or initiating claim, into the system. The process of collecting data by OCR raises a privacy risk, where individuals may not be aware that their information is being inputted into Entellitrak. This risk is mitigated as individuals are given notice that information, they are submitting will be entered into a system for further use by OCR for the purposes of responding to a claim. The Privacy Act of 1974 also provides individuals with the ability to request or amend this information, if desired.

### ***Data Minimization***

There is a risk that more than the necessary information is collected from individuals. This risk is mitigated by the general practice that CFPB always seek the minimum amount of PII necessary to complete a task related its mission. The information captured is limited to what is provided directly by individuals who contact OCR, Bureau staff records, and PII generated in response to a complaint. Individuals may choose what and how much information they share with OCR. They also have opportunities to change or update records. The initial information collected may include first name, last name, email address, and details specific to claims involving Bureau 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 contained in Entellitrak 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 registering claims and the Bureau in the event of a data breach. As a result, access to sensitive data should be limited only to CFPB staff with a need to know for their duties, excluding any unauthorized individuals (including the vendor).

CFPB minimizes this risk by enforcing access controls that limits access to data to only to authorized OCR staff. Sensitive information is only stored in systems that have the requisite security authorization for holding this type of data. Any sharing of data can only happen under authorized circumstances (i.e. referral to another government agency), to authorized individuals. 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 Bureau 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. The Bureau mitigates this risk in several ways. As a third-party system, federal standards, and regulations for safeguarding private information apply, Entellitrak must conform to CFPB security requirements, the presence of which are affirmed prior to use.

Access to the system itself and the data within it is also limited. Access controls, along with other security measures are in place to limit case file data only to OCR staff. 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 Bureau 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 within the application 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, National Institutes of Standards and Technology (NIST) controls families, including Identification and Authentication (IA) and Risk Assessment (RA), will be 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 providing 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 possible discrimination claim (by email, phone, or mail), an authorized OCR staff person collects their information (including any related PII) and enters it into Entellitrak, 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 in Entellitrak. 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 claim or otherwise involved in the claim. All information is provided voluntarily by an individual submitting the claim, however, a minimum amount of data, including PII, must be provided to identify the issue and to contact the individual making a claim for follow-up discussion and potential resolution.

If an individual chooses to pursue the EEO process, the Entellitrak case file is then assigned to an authorized OCR staff member (e.g., EEO counselor, EEO investigator, or EEO Attorney-Adviser) to manage the case. Case files can only be viewed in Entellitrak by other 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 and may ultimately make the decision as to whether discrimination occurred in violation of a civil rights law.

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 in Entellitrak. During this process, identifying information is not shared by Entellitrak nor the case manager assigned unless the individual consents, or if it is determined there is a threat of 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). OCR and OHC both use Entellitrak but each office has their own distinct and separate version of the tool (instances) and are firewalled from each other. For specific circumstances, like mandated reporting, employee data housed within OHC systems, such as demographic information, is extracted and loaded into the OCR instance of Entellitrak. OHC shares the 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 the Bureau's clearance process and published on [consumerfinance.gov](http://consumerfinance.gov) (CFPB's public website). 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](http://consumerfinance.gov). Other periodic reports may be produced in response to ad hoc inquiries. OCR data contained within the Entellitrak system may 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 stored in system by limiting it only to authorized CFPB and technical staff.

## 2. Describe CFPB's objective for the information.

OCR collects the information in Entellitrak for the administration, processing, and resolution of discrimination claims submitted by individuals who contact OCR. OCR previously used the iComplaints system for these functions. The vendor is sunsetting iComplaints, ending support and replacing it with Entellitrak's "ETK EEO". CFPB is leveraging Entellitrak to ensure continuity in its operations and to utilize the increased functionality of the new system.

OCR also uses the data within an Entellitrak case file to document claims and maintain other information that may arise while it is being reviewed. This includes any appeals or the transfer of cases to other CFPB offices or agencies. As part of the evaluation process OCR uses the case record information to investigate the claim based on applicable laws, regulations, and internal policies. Details from the case record are also used when engaging the individual and/or stakeholders who are relevant to the claim, including CFPB officials. After the conclusion of this process case files are stored in Entellitrak for record keeping.

In each stage of this process, information describing every major case "event" are documented within the case file. The objective in using this information is to assist the assessment 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. OCR collects PII in support of OCR investigative process. The PII collected is used for two primary purposes – case management, and system and EEO programmatic administration.

### *Case Management*

Entellitrak is 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 within Entellitrak when an individual contacts OCR about a potential incident. 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. A case record is created once all this has been provided. The case record is then assigned to an OCR staff member to manage the case. As more information is gathered, 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. All the available documents associated with a complaint are also stored with the case record.

The information from complainants is provided voluntarily by the individual submitting a claim and is collected to assist the individuals in addressing new issues and complaints, or existing issues and complaints that have not been appropriately addressed or have resulted in an unsatisfactory resolution. OCR may use this information in consultation with applicable laws, regulations, policy, and data to talk 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” are documented within the case record. During these processes, PII is not shared by the system nor the case manager assigned to the case unless the individual consents, or if it is determined there is a threat of 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.

### *System administration*

Entellitrak also collects and uses PII for administration of the system. PII of CFPB staff and authorized technical support from the third-party vendor is used for access and identity management of the system. Entellitrak utilizes single sign on (SSO) supported by Active Directory with a roster feed of authorized OCR CFPB staff that is updated bi-weekly. Access for Entellitrak 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 stored in Entellitrak 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, 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 strategic reflects plans to eliminate identified barriers. The Report is the result of CFPB's annual self-assessment. Aggregate and de-identified data from Entellitrak 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 claim to be initiated, collecting only a minimum amount of necessary to conduct its duties. Within CFPB, only OCR staff have access or be granted to the relevant PII associated with a claim. If the case is further pursued for a hearing at the EEOC, then it will be transferred 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 will be shared.

An assigned OCR manager can share PII from case record in Entellitrak under the following circumstances: with the individual's consent; if it is determined there is a threat of 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 providing submitting will be entered into a system for further use by OCR for the purposes of responding to a claim. 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 the Bureau'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.

Entellitrak is a vendor-hosted, cloud-based business process management tool, whose use as a third-party application is 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 is collected and the application 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. PII of CFPB staff who are involved in OCR administration or involved in the claim, is also collected, and sourced from Bureau systems.

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 Bureau cybersecurity policy and procedures
- Data Quality and Integrity Checks
- Policy and Standard Operating Procedures
- Role-based Access Controls<sup>2</sup>:

---

<sup>2</sup> Only staff from CFPB OCR will 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

- 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 Bureau 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 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.<sup>3</sup>
  - 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

This tool is not accessible to the public or anyone outside 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.

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 Bureau have access to the system, which may include authorized staff from the vendor to provide technical support. No other systems or individuals have access to the data in Entellitrak. OCR is required to create annual and quarterly reports detailing trends and measurements associated with the OCR program. Data from Entellitrak informs this document but it is not 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 is not published.

## Document control

## Approval

---

Christopher Chilbert

Chief Information Officer

Date

---

Tannaz Haddadi

Chief Privacy Officer

Date

---

Lydia Garry

Senior Advisor, Data and Programs

Date

# Change Control

| Version | Summary of material changes                 | Pages affected | Date of change |
|---------|---|----------------|----------------|
| 1.0     | New document to replace the iComplaints PIA | All            | 2/22/22        |