Enforcement Matter Management System v.3.1

Privacy Impact Assessment

June 18, 2025

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act[1] established the Consumer Financial Protection Bureau (CFPB or Bureau). The CFPB is a 21st century agency that implements and enforces Federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive.

A central part of the Bureau's mission is to protect consumers and make sure they are treated fairly in the financial marketplace. One way the CFPB does this is by enforcing federal consumer financial laws and holding financial service providers accountable for their actions. Pursuant to sections 1052, 1053, and 1054 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5562-5564[2] the CFPB's Enforcement Division (Enforcement) is authorized to conduct investigations, issue civil investigation demands, initiate administrative adjudications, and initiate public enforcement actions in state and federal court against persons[3] (hereinafter referred to as "entities and individuals") for engaging in conduct that may violate rules and/or statutes within the CFPB's authority.

The CFPB also coordinates with other federal or state agencies (e.g., Federal Trade Commission (FTC), Office of the Comptroller of the Currency, Department of Justice, and state

---

[1] Public Law No. 111-203, Title X.

[2] The Bureau's enforcement authority varies by the particular statute being enforced.

[3] The rules governing enforcement investigations under section 1052 of the Dodd-Frank Act, 12 U.S.C. § 5562, apply to a "person" as defined in 12 C.F.R. Part 1080.This term encompasses individuals as well as partnerships, companies, corporations, associations (incorporated or unincorporated), trusts, estates, cooperative organizations, or other entities, as specified in 12 C.F.R. § 1080.2. In contrast, "individuals", as defined under the Privacy Act of 1974, are typically U.S. citizens and lawful permanent residents. 5 U.S.C. §552a (a)(2). This definition does not extend to an entity that is not a natural person, such as partnerships, companies, corporations, associations (whether incorporated or unincorporated), trusts, estates, or cooperative organizations. However, non-natural entities such as corporations are considered legal "persons" and can be held liable similarly to individuals. Therefore, they may also be identified in an enforcement investigation and held liable for consumer financial law violations.

Additionally, the Bureau's ability to enforce the Consumer Financial Protection Act (CFPA), including its prohibition on unfair, deceptive, or abusive acts and practices, is limited to "covered persons" and "service providers." 12 U.S.C. §§ 5531(a), 5536. "Covered person" includes "any person that engages in offering or providing a consumer financial product or service." "Service provider" includes "any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service." The CFPA also extends to persons who "knowingly or recklessly provide substantial assistance." Other federal consumer financial laws are broader and apply to "any person," subject only to the limitations in Subtitle B of the CFPA.

Attorneys General) to inform related work and reduce the burden on institutions that are the subject of an enforcement investigation.

Enforcement is responsible for tracking, managing, and taking appropriate action in accordance with the CFPB's enforcement authority. Enforcement uses a suite of applications within the Enforcement Matter Management System to track and manage activity regarding potential, pending, and closed enforcement matters (e.g., investigations and litigations, including public enforcement actions) for administrative purposes, as provided in Public Law 111-203, Title X, Sections 1011, 1012, 1021, and 1054 codified at 12 U.S.C. §§ 5491, 5492, 5511, and 5564. The system is hosted in CFPB's Salesforce environment.[4] Salesforce provides a cloud-based solution that allows the CFPB to develop and implement enterprise applications that focus on customer service, project management, and analytics.

Enforcement Matter Management System matter records include relevant details about the enforcement matter, both descriptive and administrative in nature. The system allows users to create, track, manage, and report on enforcement matters throughout their lifecycle. Specifically, the Enforcement Matter Management System enables users to:

- Create potential and new enforcement matter records;
- Record activities and track historic details, including CFPB Staff[5] associated with enforcement matters;
- Upload and link to key documents; and
- Report out on information contained within the system.

Information in a matter record varies depending on the stage and complexity of the enforcement matter. Matter records and their accompanying documents may contain personally identifiable information (PII) about individuals, including CFPB Staff, other federal or state agency employees, and members of the public. Generally, a matter record may include the following information:

- Information about related entities and individuals, such as the institution name, address, phone number, website, and fax number, in addition to the Taxpayer Identification Number

---

[4] *See* CONSUMER FINANCIAL PROTECTION BUREAU, SALESFORCE AND PLATFORM CLOUD ENVIRONMENT PRIVACY IMPACT ASSESSMENT (April 2022) and subsequent updates, *available at*, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[5] CFPB Staff means all employees, interns, volunteers, contractors, and detailees assigned to CFPB.

(TIN) which will be used to identify an entity for the CFPB to comply with its federal tax reporting obligations;

- Limited information related to applicable supervisory events, such as CFPB-issued exam identification numbers, or the nature or summary of the exam;
- CFPB Staff contact information associated with each matter;
- Names and contact information of certain members of the public such as, individuals associated with a related entity (e.g., directors, officers and employees); recipients of civil investigative demands (CIDs); opposing counsel; potential witnesses; experts; relevant consumers; related federal, state, and local government employees; and judges;
- Stage of the matter (e.g., pre-investigation, investigation, litigation);
- Deadlines and important dates for each matter;
- Public Actions, petitions, and other litigations related to the matter;
- Final dispositions; and
- Copies of or links to key documents in Enforcement's document storage system. Such documents may include CIDs, Opening and Closing Memos, Sue/Settle Memos, and Investigation Plan documents. Other documents associated with a matter are primarily stored in a separate system and may be linked to the matter record. These documents include data, information, and documents relevant to the specific matter, such as, legal memoranda, consumer complaints, whistleblower tips, responses to CIDs, transcripts, correspondence, and legal filings.

The information and records maintained in the Enforcement Matter Management System are covered by the System of Records Notice (SORN) CFPB.004, Enforcement Database. [6] Additionally, the system may collect and maintain, or share records with other CFPB systems that are subject to different SORNs such as CFPB.002, CFPB Supervision and Examination Records

[6] *See* CFPB.004—ENFORCEMENT DATABASE, 88 Fed. 7690 (Feb. 06, 2023) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

SORN[7]; CFPB.018, CFPB Litigation Files,[8] and CFPB.025, Civil Penalty Fund and Bureau-Administered Redress Program Records.[9]

Furthermore, access account records for CFPB Staff and external authorized system users are covered under the CFPB.014, Direct Registration and User Management System (DRUMS) SORN.[10] The CFPB.009, Employee Administrative Records SORN[11] covers CFPB Staff training records and the General Services Administration (GSA)/GOVT-10, Federal Acquisition Regulation Data Collection System SORN [12] provides coverage for CFPB contractors, subcontractors, and their employees.

The original Privacy Impact Assessment (PIA) for the Enforcement Matter Management System—previously known as the Matter Management System PIA—was published on May 24, 2012, was updated on October 22, 2012, and again on October 22, 2024. The PIA described how the Bureau created the Matter Management System, a central searchable repository of information relating to each matter that enabled Enforcement to organize and distribute information about each matter to those authorized to know, track key dates for each matter, report on administrative and statistical information about each matter, and develop and record plans for conducting matters, including identifying personnel resources necessary to conduct each matter.

The 2024 PIA update documented the migration of the Matter Management System into CFPB's Salesforce environment and the addition of a new application and module, which collectively are referred to as the Enforcement Matter Management System. This system includes

---

[7] *See* CFPB.002 SUPERVISION AND EXAMINATION RECORDS, 89 Fed. Reg. 73077 (Sept. 9, 2024) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

[8] *See* CFPB.018—CFPB LITIGATION FILES, CONSUMER FINANCIAL PROTECTION BUREAU, 83 Fed. 23435 (May 21, 2018) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

[9] *See* CFPB.025—CIVIL PENALTY FUND AND BUREAU-ADMINISTERED REDRESS PROGRAM RECORDS, 83 Fed. 23435 (May 21, 2018) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

[10] *See* CFPB.014—CFPB DIRECT REGISTRATION AND USER MANAGEMENT SYSTEM, 83 Fed. 23435 (June 21, 2018) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

[11] *See* CFPB.009—CFPB EMPLOYEE ADMINISTRATIVE RECORDS, 85 Fed. 48510 (Aug. 11, 2020) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

[12] *See* GSA/GOVT-10 FEDERAL ACQUISITION REGULATION DATA COLLECTION SYSTEM, 82 FR 12352 (Mar. 2, 2017) *available at,* https://www.gsa.gov/reference/gsa-privacy-program/systems-of-records-privacy-act/system-of-records-notices.

the ENForce and ENFund applications, and the CFPB-FTC Matter Sharing Community module. The primary application within the system is ENForce, which includes the functionality of the previous Matter Management System. The ENFund application is a financial management tool that allows Enforcement to track financial requests, approvals, commitments, obligations, and expenditures against the budget at the matter level, and as applicable, the individual level (e.g., training requests for CFPB Staff). Also included in the system is the CFPB-FTC Matter Sharing Community module, which is a secure portal that allows for the sharing of certain, limited information about enforcement matters with the FTC to facilitate the coordination of law enforcement activities consistent with the operative Memorandum of Understanding.[13] The Enforcement Matter Management System will also be integrated with Enforcement's document storage system to limit the duplication of records and information.

The CFPB is publishing this updated PIA to document the collection and use of the TIN for transparency. This PIA update also includes non-substantive changes that do not impact PII or privacy.

Privacy Analysis and Risk Management

The CFPB conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[14] and in alignment with Office of Management and Budget[15] (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures for the Enforcement Matter Management System, pursuant to the Fair Information Practice Principles. This includes the design and implementation of administrative, technical, or physical safeguards or controls, as applicable.

1. Characterization of Information

[13] MEMORANDUM OF UNDERSTANDING BETWEEN THE CONSUMER FINANCIAL PROTECTION BUREAU AND THE FEDERAL TRADE COMMISSION (Feb. 25, 2019).

[14] 44 U.S.C. § 3501 note.

[15] Although pursuant to section 1017(a)(4)(E) of the Dodd Frank Wall Street Reform and Consumer Financial Protection Act, Public Law 111-203, the CFPB is not required to comply with OMB-issued guidance, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

1.1 Identify the information the CFPB collects, uses, disseminates, or maintains, and the individuals about whom the information pertains.

As noted above, Enforcement staff collect and enter a limited amount of information into the Enforcement Matter Management System related to enforcement matter activities. This data may include:

- Information about CFPB Staff such as first and last name, title, business contact information (e.g., office address, phone number, and email address), role in an enforcement matter, and potential conflicts of interest with regulated entities as voluntarily submitted;
- Information about entities currently or previously associated with CFPB enforcement matters, such as entity name, contact information (e.g., mailing address, phone number, fax number, and website address), and TIN when necessary for the CFPB to meet its tax reporting obligations[16];
- Information about individuals who are or were associated with CFPB enforcement matters, such as first and last name, and contact information. These individuals include members of the public who are or were associated with a related entity (e.g., directors, officers and employees); recipients of CIDs; opposing counsel; potential witnesses; experts; relevant consumers; related federal, state, and local government employees; and judges;
- Copies of or links to key documents in Enforcement's document storage system. These documents may include CIDs, Opening and Closing Memos, Sue/Settle Memos, and Investigation Plan documents.

ENFund Application

The ENFund application functionality broadens the number and types of contractor information collected in the Enforcement Matter Management System and adds new functions that collect additional information pertaining to CFPB Staff. The system collects a limited amount of information on these entities and individuals, including:

- Name and business contact information for vendors and contractors (e.g., trainers, court reporting companies, general suppliers, and experts and their staff);
- Information related to contracts (e.g., contract number, cost) and contractors, including performance records; and

[16] *See* 26 U.S.C. § 6050X.

- Information about trainings requested and/or attended by CFPB Staff (e.g., training name, location, and vendor, including vendor contact information).

CFPB-FTC Matter Sharing Community Module

The CFPB-FTC Matter Sharing Community module is a portal that allows authorized users at the FTC to input and edit FTC enforcement matters into a secured module within the Enforcement Matter Management System. The FTC enforcement matter records can be accessed by authorized CFPB Staff through ENForce as needed. The FTC enforcement matter records may include:

- Names and contact information (e.g., email, phone number) of FTC staff associated with the FTC enforcement matter;
- Names of potential subject or defendant entities and individuals who are or were associated with the FTC enforcement matter; and
- URL links to other relevant public information related to the FTC enforcement matter.

1.2 What are the sources of information and how is the information collected?

Enforcement relies on a number of sources of information to identify potential activities that may warrant opening an investigation, including:

- Consumer complaints;
- The Bureau's whistleblower hotline;
- Referrals from federal regulators and other local, state, and federal agencies;
- Market intelligence; and
- The results of supervisory exams.

The Bureau's Enforcement Director or one of their deputies approve opening a Bureau investigation. In assessing whether to open an investigation, Enforcement weighs a number of factors, including, but not limited to, whether:

- There is a plausible set of facts that, if proven, would amount to a violation of one or more federal consumer financial laws;
- There is reason to believe that one or more specific entities may be engaging in the conduct described in those facts;
- There is evidence of a magnitude of harm that justifies investment of resources;
- There are sufficient resources available to properly address the matter; and

- The devotion of those resources is consistent with the strategic planning and articulated priorities or warrants a conscious departure from those plans and priorities.

The existence of an investigation does not mean that the individual or entity has violated the law.

In conjunction with an enforcement matter, CFPB Staff may collect information directly from entities (including employees of an entity) or individuals who are the subject of or related to an enforcement matter, from consumers including through the CFPB's and/or the FTC's consumer complaint databases,[17] and from other state or federal agencies responsible for related regulatory functions. CFPB Staff may collect information through documents that entities and individuals submit to the CFPB, such as financial disclosure forms, and through CIDs and other legal discovery processes, including investigational hearings, depositions, interrogatories, requests for production of documents, and requests for admission. Additionally, CFPB Staff may collect and use information available and obtained through state and federal data sources (e.g., HMDA data, Secretary of State websites), commercial sources, or other publicly available information, such as legal research tools authorized for use by CFPB that streamline public records searches.

The information collected through the ENFund application is collected directly from CFPB Staff and vendors.

Finally, FTC Staff authorized to access the CFPB-FTC Matter Sharing Community module have the capability to create, update, and upload relevant documents to FTC enforcement matter records. This data is shared with authorized CFPB users through ENForce as needed to facilitate the coordination of law enforcement activities consistent with the Memorandum of Understanding (MOU).[18]

1.3 If the information collection is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number for the collection.

The information maintained in the Enforcement Matter Management System is not subject to the Paperwork Reduction Act (PRA) requirements because these collections fall under the exception to coverage of the PRA found at 5 C.F.R. 1320.4 (a) (1), (2), and (3).

---

[17] *See* the CFPB CONSUMER RESPONSE SYSTEM PRIVACY IMPACT ASSESSMENT (Aug. 2024) available at, https://www.consumerfinance.gov/privacy/privacy-impact-assessments/; the FTC SENTINEL NETWORK SERVICES PRIVACY IMPACT ASSESSMENT (Mar. 2023), and subsequent updates. For more information regarding the FTC's Consumer Sentinel, please visit https://www.ftc.gov/policy-notices/privacy-policy/privacy-impact-assessments.

[18] MEMORANDUM OF UNDERSTANDING BETWEEN THE CONSUMER FINANCIAL PROTECTION BUREAU AND THE FEDERAL TRADE COMMISSION (Feb. 25, 2019).

1.4 Discuss how the accuracy of the information is ensured.

Enforcement updates the information in the Enforcement Matter Management System as matters progress. When practicable, this includes confirming names and other PII of certain external entities and individuals associated with matters. Such information may include, mailing address, phone number, email address or website, and an individual's entity affiliation.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that information in the Enforcement Matter Management System is used for purposes beyond those described in this PIA.

Mitigation: To mitigate this risk, CFPB Staff that require elevated privileges to complete their job functions must sign and electronically submit the *Privileged User Access (PUA) Form* to obtain elevated access to the Enforcement Matter Management System and review and acknowledge the *Rules of Behavior for Privileged Users*. The rules of behavior define the user's responsibilities, such as confirming that they will protect information from misuse and ensure information is only disclosed to authorized individuals that have a need to know. All CFPB Staff are required to only share information externally when permitted by the CFPB's rules governing the Disclosure of Records and Information.[19]

Additionally, all CFPB Staff with access to CFPB systems, such as the Enforcement Matter Management System, must sign the CFPB "Acceptable Use of CFPB Information Technology Resources" policy. This policy establishes the user's responsibilities and the requirements to safeguard information technology resources and information. This includes protecting PII and other sensitive or confidential information. Finally, all CFPB Staff are required to take annual privacy training. CFPB privacy training stresses the importance of the appropriate and authorized use of personal information in government information systems.

2. Limits on Information Collection and Retention

2.1 Explain how the CFPB only collects and maintains the information that is directly relevant and necessary to accomplish the specified purpose(s).

CFPB only collects information that is relevant and necessary to investigating potential violations of federal consumer financial law and pursuing administrative or civil enforcement

[19] *See* 12 CFR 1070, DISCLOSURE OF RECORDS AND INFORMATION, 78 Fed. Reg. 11483 (Mar. 18, 2013).

actions. The information collected and maintained in the Enforcement Matter Management System allows CFPB Staff to manage investigations and litigation by tracking the activity of an enforcement matter throughout the matter lifecycle.

In addition, PII collected through the ENFund application includes contact information for vendors, and contractors, as well as other sensitive information related to the contract (e.g., performance records). This information collection is necessary to manage contracts and track spending for Enforcement. Associating it with matters enables Enforcement to track financial requests, approvals, commitments, obligations, and expenditures against the program budget at the matter level. Also, individual training requests are tied to CFPB Staff records.

Finally, authorized FTC Staff may input and edit FTC enforcement matter records in the CFPB-FTC Matter Sharing Community module. This limited information on FTC enforcement matters is designed to support coordination between the CFPB and FTC, consistent with the governing coordination MOU.

2.2 Describe the records retention requirements for the information. Has the retention schedule been approved by the CFPB and the National Archives and Records Administration (NARA)? If so, include the retention schedule.

Records maintained in the Enforcement Matter Management System are retained and disposed of in accordance with National Archives and Records Administration (NARA) approved Enforcement Records schedule. If the record is being used for a specific matter, then it becomes a matter record and is subject to the disposition schedule as it applies to that matter, which can range from one year beyond the year created to permanently archived for historically significant cases. Per NI-587-12-8, records will be destroyed 15 years after cutoff.

Privacy Impact Analysis: Related to Limits on Information Collection and Retention

Privacy Risk: There is a risk that authorized users collect more information than is necessary for enforcement matters.

Mitigation: To mitigate this risk, the CFPB has established technical controls and privacy safeguards to collect only a limited amount of information about individuals that is narrowly tailored to effectively track and manage the enforcement matter lifecycle. For example, the ENForce application data fields are limited to information relevant to enforcement matters, limiting PII in the system.

In addition, only authorized users may create and/or edit Enforcement Matter Management System records. Authorized users may also add documents that might contain PII to a system

record. However, these documents are limited to key documents that are relevant to the management and tracking of an enforcement matter.

Finally, future enhancements to the Enforcement Matter Management System will also limit the collection of information maintained in the system. For example, integrating the ENForce and ENFund applications with other systems where relevant information and documents are maintained, such as in the matter document library, or in other CFPB systems, will prevent the duplication of information and/or documents across CFPB systems.

3. Uses of Information

3.1 Describe the purpose of the information and how the CFPB uses it.

The CFPB uses the information collected and maintained in the Enforcement Matter Management System to manage various types of activity related to potential, pending, and closed enforcement matters. The ENForce application is used to track, search, and report on enforcement matter details, including:

- The stage of enforcement matters, associated dates, and documentation of authority;
- Related individuals and entities;
- The assignment of matters to CFPB Staff;
- Civil investigative demands issued, and associated deadlines;
- Deadlines and planning associated with enforcement investigations and litigations, and associated tolling agreements;
- Processing of incoming and outgoing information;
- Interagency access requests and the timing of responses;
- Experts and other professionals considered or engaged in conjunction with enforcement matters;
- Public enforcement actions and related litigations and associated final dispositions;
- Certain tax information required by the Internal Revenue Service (IRS)[20]; and
- Status of legal holds and associated individuals.

[20] See 26 U.S.C. § 6050X.

In addition, the ENFund application streamlines business processes, making it easier to track and monitor spending effectively, and to allow for meaningful analysis and reporting. Specifically, the ENFund application allows:

- Enforcement staff to initiate requests for matter-related expenditures, including contractors, experts, and other necessary goods and services, linking them to specific matters;
- Enforcement staff to initiate requests for training;
- Enforcement Supervisors and operations staff to approve requested expenditures;
- Enforcement staff to leverage system data to initiate requests for court reporting services;
- Enforcement operations staff to track contracts, including commitments, obligations, invoices, expenditures, and contractor performance;
- Enforcement staff to track all purchase card purchases, including receipts; and
- Enforcement operations staff to track expenditures against Enforcement's budget and budget lines within and across fiscal years.

3.2 Is the information used or shared with other CFPB programs, systems, or projects?

The CFPB may generate various reports from the Enforcement Matter Management System that identify enforcement matters, related entities and individuals including CFPB Staff, and different elements of the matter. The amount or type of information in these reports, including PII, varies depending on the purpose of the report. For example, some reports may include confidential information about the status of a matter. Other reports may include aggregate or specific information about public enforcement actions, such as filing dates or monetary amounts ordered. In other cases, reports containing aggregated or de-identified data (i.e., reports that do not contain PII) may be generated to help inform and prioritize the Bureau's market-monitoring efforts, including research regarding risks to consumers presented in particular markets. The ENFund application allows staff to generate reports on Enforcement's spending. The CFPB distributes reports derived from the system internally only to CFPB Staff with a need to know to carry out their assigned job responsibilities.

For the purposes of internal CFPB coordination, certain other CFPB Staff, who have a demonstrated need to know, have limited access to the ENForce application (e.g., T&I, Legal, Supervision, Markets, and Regulations). Some entity and individual information (e.g., name,

contact information, TIN) is also shared with the Supervision Division's (Supervision) Supervision and Examination System (SES).[21]

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that CFPB may use information in the Enforcement Matter Management System in a manner inconsistent with the intended purpose for which it was collected or shared with those who do not have a need to know.

Mitigation: To mitigate this, the CFPB shares information in accordance with the SORNs identified above. Generally, access to matter records is limited to authorized CFPB Staff. A limited number of authorized FTC users have access to a very limited set of CFPB data (discussed in detail below). Additionally, there is a risk that information may be inadvertently shared with another application within Salesforce. The CFPB mitigates this risk by using the Salesforce application in accordance with its Authority to Operate (ATO) based upon the CFPB Approved and Authorized (A&A) processes. The CFPB assesses A&A connections between applications to apply role-based environment access controls to ensure the security and privacy of the interconnection. The CFPB also assesses proposed data sharing between the cloud environments to ensure only authorized users access matter records. The CFPB also configures security controls at a granular level within each application to prevent sharing PII externally.

4. Individual Notice and Participation

4.1 Describe what opportunities, if any, individuals to whom the information pertains receive notice prior to the collection of information. If notice is not provided, explain why not.

General notice is provided by the CFPB through its rulemakings, this PIA, and applicable SORNs. Generally, employees and consumers of entities and individuals do not receive prior notice because Enforcement often does not collect the information directly from the individual. For example, most of the information collected within the ENForce application is provided by entities and individuals, or their representatives, pursuant to applicable laws and regulations.

Additionally, Title V, Subtitle A of the Gramm-Leach-Bliley Act (GLBA) and Regulation P, which implements the GLBA, mandate that financial institutions provide their customers (e.g., borrowers) with privacy notices regarding those institutions' privacy policies and practices.

[21] *See* CONSUMER FINANCIAL PROTECTION BUREAU, PRIVACY IMPACT ASSESSMENT FOR THE SUPERVISION AND EXAMINATION SYSTEM (SES) (May 2023), available at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

Among other requirements, Regulation P requires that these privacy notices describe the conditions under which the financial institution may disclose nonpublic personal information about customers to nonaffiliated third parties.[22] These privacy notices may be provided annually, directly to customers, or posted on the financial institution's website.

4.2 Describe what opportunities are available for individuals to consent to use, decline to provide information, or opt out of the CFPB's collection and use of the information.

As noted above, individuals typically do not have an opportunity to opt out or decline to provide information that is maintained in the Enforcement Matter Management System because information is often not collected directly from the individual. As exemplified above, information about employees and consumers of entities and individuals collected within the ENForce application is provided by those entities pursuant to applicable laws and regulations. However, in some instances CFPB Staff may collect information directly from individuals who are the subject of or related to an enforcement matter, such as from consumers through the CFPB's consumer complaint process who voluntarily provide this information to the CFPB.

4.3 What are the procedures that allow individuals to access their information or correct inaccurate information?

Regardless of citizenship, individuals may seek to access or correct their information maintained in the Enforcement Matter Management System through the CFPB's Freedom of Information Act (FOIA) Office in writing in accordance with the Bureau's Disclosure of Records and Information Rules, Subpart E-Privacy Act [23] promulgated at 12 C.F.R. 1070.50 *et seq.* If you have any questions, please contact the CFPB FOIA Office via FOIA@CFPB.gov or at (855) 444-3642.

All or some of the information requested may be exempt from access pursuant to the Privacy Act of 1974[24] or FOIA to prevent harm to an investigation or enforcement action. Providing

---

[22] 12 C.F.R. Part 1016 *et. seq*. Title X of the Dodd-Frank Act Wall Street Reform and Consumer Protection Act granted rulemaking authority for most provisions of Title V, Subtitle A of the GLBA to the CFPB concerning entities and individuals subject to the CFPB's jurisdiction, except securities and futures-related companies and certain motor vehicle dealers. The Dodd-Frank Act also granted authority to the CFPB to examine and enforce compliance with these statutory provisions and their implementing regulations concerning entities under CFPB jurisdiction.

[23] eCFR :: 12 CFR Part 1070 -- Disclosure of Records and Information

[24] 5 U.S.C. § 552a.

individuals with access to these records could inform the subject of an actual or potential investigation or reveal investigative interests on the part of CFPB or another government agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, such as by tampering with witnesses or evidence.

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that individuals are not aware of or will not have the opportunity to consent to the collection of their information maintained in the Enforcement Matter Management System.

Mitigation: This risk cannot be mitigated. As noted above, individuals typically do not have opportunities to opt out or decline to provide information that is maintained in the Enforcement Matter Management System because Enforcement often does not collect the information directly from the individual. For example, the CFPA specifically requires subjects of Bureau CIDs to provide *all* information requested.[25] Such information includes all information relevant to any violation of consumer financial law. [26] Therefore, during an enforcement investigation, Enforcement may collect information about individuals through third party entities and individuals.

5. External Sharing and Disclosure of Information

5.1 Does the CFPB share this information with external entities or partners? If so, identify the organization or third-party and how the information is accessed and used.

Information maintained in the Enforcement Matter Management System is shared in accordance with all laws, regulations, policies, and applicable CFPB SORNs, or in response to FOIA requests. As noted above, the CFPB established the CFPB-FTC Matter Sharing Community module to provide authorized FTC Staff the ability to input and edit FTC matter records, upload documents to FTC matter records, and search and view a limited set of data from CFPB enforcement matter records. The purpose for sharing information with the FTC is to coordinate law enforcement activities, prevent the duplication of efforts, avoid placing unnecessary burdens on entities, and ensure there is consistent enforcement of federal consumer financial laws where

[25] *See* 12 USC 5562(c)(10).

[26] See 12 USC 5562(c)(1).

there are overlapping legal and regulatory authorities.

Additionally, a limited amount of information collected through the ENFund application is shared with court reporting vendors, specifically witness names and entity affiliation, as well as names, addresses, and other business contact information for opposing counsel, and CFPB Staff. Court reporting services are required when taking testimony (investigational hearings and depositions); the PII sharing is necessary for scheduling and documenting participants.

The CFPB also reports to the IRS information regarding certain fines, penalties, and other amounts levied against entities and individuals resulting from the CFPB's lawsuits and settlements. The sharing of certain PII, such as TIN, with the IRS is necessary for meeting these reporting requirements.

5.2 Does the CFPB place limitations on information sharing and/or re-dissemination of the information?

Limited information is shared with designated FTC Staff through the CFPB-FTC Matter Sharing Community module, who may not further disclose the information, except as set forth in the applicable MOU. Enforcement also ensures information it discloses to third parties is subject to appropriate protections, such as through a protective order or MOU.

Privacy Impact Analysis: Related to External Sharing and Disclosure of Information

Privacy Risk: There is a risk that information maintained within the Enforcement Matter Management System may be accessed by unauthorized individuals who do not have a need to know or used in a manner that is inconsistent with the purpose for collection.

Mitigation: To mitigate this risk, Enforcement has implemented administrative, technical, and physical safeguards to protect the Enforcement Matter Management System and the information collected and maintained therein. For example, designated FTC staff need a user account to access the CFPB-FTC Matter Sharing community module, and the module itself only contains limited information. FTC user account requests must be submitted to and approved by FTC and Enforcement staff before system administrators create an FTC user account. Approved FTC users receive a welcome email directing them to create a username and password and use multi-factor authentication to access the CFPB-FTC Matter Sharing Community module.

As a federal database, the CFPB-FTC Matter Sharing Community module is subject to the Federal Information Security Modernization Act (FISMA), which requires the annual verification that all users who access federal systems have both the business need and the authorization to access the system. To comply with FISMA, government users must annually verify employment and that their role requires continued access to the system. Enforcement staff are responsible for

granting access to the CFPB-FTC Matter Sharing Community module and will terminate access for FTC Staff in accordance with all policies and protocols.

Finally, the CFPB-FTC Matter Sharing Community module generates audit logs of user activity, including FTC users, to monitor unusual system behavior. Audit logs track when FTC users are logged onto the system, who views which records, who uploads documents to an FTC matter record, and how records are used within the system (e.g., unauthorized creation, system configurations). Any evidence of misuse may result in the termination of the FTC user account.

6. Accountability, Auditing, and Security

6.1 How does the CFPB secure the information to ensure that it is used in accordance with stated practices in this PIA?

The CFPB complies with the Privacy Act, the Right to Financial Privacy Act, and the E-Government Act of 2002, Section 208. To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopted the Fair Information Practice Principles (FIPPs) as the framework for its privacy policy. The FIPPs apply throughout the CFPB for the collection, use, maintenance, disclosure, and destruction of PII, and any other activity that impacts the privacy of individuals, regardless of citizenship, to ensure compliance with all laws, regulations, and policy requirements.

The CFPB adheres to the Office of Management and Budget (OMB) privacy-related guidance [27] and applies the National Institute of Standards and Technology (NIST) Risk Management Framework for information technology systems, applications, solutions, and services.[28] The NIST RMF identifies processes for the identification of NIST SP-800-53 security and privacy controls and continuous monitoring of controls to ensure on-going compliance.[29]

6.2 Describe what privacy training is provided to users either generally or specifically relevant to CFPB information system.

---

[27] More information regarding OMB guidance is available at, https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/.

[28] *See* NIST Risk Management Framework (RMF) For Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, SP-800-37 Revision (Rev). 2 (December 2018). For more information visit https://www.nist.gov.

[29] *See* NIST Security and Privacy Controls for Information Systems and Organizations, SP-800-53, Rev. 5 (September 2020). For more information visit https://www.nist.gov.

All CFPB Staff are required to adhere to all CFPB cybersecurity and privacy policies and take mandatory annual training. For example, CFPB Staff are required to take the CFPB Privacy Training and Security Awareness Training within thirty days of their onboarding and annually thereafter. The privacy training ensures that CFPB Staff understand their responsibilities to safeguard PII and to identify and report suspected or confirmed privacy breaches within twenty-four hours of discovery. CFPB Privacy Office is notified of CFPB Staff that fail to complete the annual privacy training, at which time, their access is terminated until their annual privacy training is complete.

6.3 What procedures are in place to determine which users may access CFPB information systems and how the CFPB provides access?

CFPB Staff with access to CFPB information and systems and facilities are required to proceed through background investigations for suitability and security clearance determinations before onboarding. This ensures compliance with all federal laws and that individuals supporting the CFPB are deemed reliable, trustworthy, and suitable for the role they will fulfill. Other requirements placed on federal contractors may also include those associated with Federal Acquisition Regulations.

CFPB Staff must properly obtain and present credentials to gain access to CFPB facilities and systems. The CFPB's secure access controls policy, "Secure Access Controls via Multi-Factor Authentication" Policy applies to CFPB Staff that have logical and/or physical access to CFPB facilities, information systems or applications, and/or information (in physical or electronic form). This ensures the CFPB maintains a secure operating environment and protects our systems against potential external threats.

In addition, the CFPB employs role-based access controls to ensure users only have access to the system and/or information necessary and relevant to their assigned duties. For example, different CFPB users may be granted varying levels of access to the information within the Enforcement Matter Management System (e.g., limited view of a matter, full view of the matter including uploaded documents) and functionality (read-only access, ability to edit) based on their specific role. The Enforcement Matter Management System Product Owners are authorized to grant Enforcement Staff and other CFPB program offices Staff (e.g., Supervision, Legal, etc.) varying levels of access to the system based on the user's role within the CFPB. Individuals who no longer require access have their credential removed from the system.

Privacy Impact Analysis: Related to Accountability, Auditing, and Security

Privacy Risk: There is a risk that unauthorized users may access the Enforcement Matter Management System or information maintained therein.

Mitigation: To mitigate this risk, the CFPB has implemented the above technical, physical, and administrative controls to safeguard PII and other sensitive information maintained in the Enforcement Matter Management System. For example, internal access to the system is limited to CFPB Staff that have a need to know. As noted above, CFPB Staff cannot access the system without being granted access by the system's Product Owners.

In addition, the CFPB has established oversight controls through robust auditing features to identify and support accountability for unauthorized use/misconduct. CFPB's "Information Governance" Policy outlines the established rules on the intake, management, disclosure, and disposition of information (in its various formats) at CFPB and applies to all CFPB users. CFPB Staff are required to review and sign the CFPB's "Acceptable Use of CFPB Technology Resources Policy" and complete the privacy and security training within thirty days of their onboarding, and annually thereafter, to maintain access to a CFPB system.

Suspicious and/or unauthorized access is monitored and logged, thereby discouraging users from inappropriate access to CFPB systems. Security administrators review audit logs of the system and applications identified herein to monitor for unusual behavior (e.g., disabling security, login times, number of login attempts, failed login attempts) or misconduct (e.g., unauthorized removal of data) by authorized users. For example, the CFPB employs extract logging and 90-day reviews to identify user behavior and Staff actions around particular events within the Enforcement Matter Management System, such as changes in the information or data, warnings, or errors that are unexpected, which are reviewed in relation to their job roles and workflow.

If the system administrator notices that anyone has used a system in violation of CFPB policy, system access may be revoked. If there is evidence of potential misconduct, the incident will be referred to the appropriate Bureau office for investigation and further review. CFPB Staff will be disciplined accordingly, which could include adverse actions or removal from the CFPB.

Document Control

Approval

Chris Chilbert
Chief Information Officer

Kathryn Fong
Chief Privacy Officer

Aaron Jeschke
Product Owner

Darcie Polzien
Product Owner

Danny Pham
System Owner

Original, signed document on file with the CFPB Privacy Office.