Enforcement Whistleblower Tip Database Application PIA v.2

Privacy Impact Assessment

September 2026

Consumer Financial
Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act)[1] established the Consumer Financial Protection Bureau (CFPB or Bureau). The CFPB works to create and support innovative and resilient consumer financial markets where consumers can choose the products and services that meet their individual needs.

The original Privacy Impact Assessment (PIA) for the Enforcement Whistleblower Tip Database Application was published on December 10, 2020. This update addresses the addition of transcription software for voicemail messages left on the whistleblower tip line voicemail box and conforms with the CFPB's newest PIA template.

A central part of the Bureau's mission is to identify conduct that may potentially violate any federal consumer financial laws or rules within its jurisdiction and to take appropriate action.[2] One of the ways the CFPB achieves this is through the collection of information from various sources, including whistleblowers who may voluntarily report potential industry misconduct to the Bureau's Enforcement Division (Enforcement).[3] Whistleblowers may include members of the public, consumers, current or former industry employees, or industry insiders.[4]

To facilitate the collection of information from whistleblowers, Enforcement uses the Whistleblower Tip Database (WTD) application to electronically collect and maintain information voluntarily submitted by whistleblowers (by phone, mail, or email), and to create records of the tips for processing by Enforcement staff[5] in an efficient and accurate manner. The WTD

---

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

[2] *See* 12 U.S.C. §§ 5491, 5492, 5511.

[3] *See* https://www.consumerfinance.gov/enforcement/information-industry-whistleblowers/

[4] Whistleblowers who are covered employees or any authorized representative of a covered employee are entitled to certain protections. *See* 12 U.S.C. § 5567. Covered employee means any individual performing tasks related to the offering or provision of a consumer financial product or service. 12 U.S.C. § 5567(b).

[5] Enforcement staff is limited to Enforcement employees and contractors.

application allows Enforcement to consolidate, track, task, and manage tip records, and to create real-time routine and ad hoc reports to aid in determining appropriate action, if any.

When providing tip information, whistleblowers decide what to share because the Bureau does not require specific data elements or personally identifiable information (PII) in whistleblower tip submissions. The whistleblower may choose to include PII, typically name, job title, and contact information, or submit a tip without providing any PII. If contact information is submitted with the tip, Enforcement may maintain the information to contact the individual, as needed and appropriate, to facilitate its analysis of the tip and determine appropriate subsequent investigative activities or action, if any. In the exceedingly rare instances when Social Security numbers (SSNs) are provided and the tip is actionable, Enforcement intake staff[6] redact the SSN before routing the tip for further access or review.

The CFPB may also use the tip information and PII to support the Bureau's enforcement[7] and supervisory activities that include investigation and examination of covered persons or service providers' practices for potential violations of federal consumer financial law. To that end, Enforcement may share tip information without PII with the Supervision Division (Supervision).[8]

Tip information may also include PII pertaining to a third-party individual affiliated with the entity (*e.g.,* an employee at a financial institution) that is the subject of the tip. Third-party PII may also be used to support the Bureau's enforcement and supervisory activities. Given the nature of the tip, third-party individuals identified within the tip information are not typically made aware that their PII was submitted by a whistleblower. The CFPB may also share whistleblower and

---

[6] Enforcement intake staff consist of Enforcement employees with permissions to access tip submissions at the time of intake. Intake staff are a subset of the Enforcement staff with access to the WTD application.

[7] The Bureau's enforcement authority varies by the particular statute being enforced. Pursuant to sections 1052, 1053, and 1054 of the Dodd-Frank Act, 12 U.S.C. §§ 5562-5564 the CFPB's Enforcement Division is authorized to conduct investigations, initiate administrative adjudications, issue civil investigation demands, and initiate public enforcement actions in state and federal court against persons for engaging in conduct that may violate rules and/or statutes within the CFPB's authority.

[8] Please see the Supervision, Enforcement, and Fair Lending Data PIA for a discussion of the Bureau's collection and use of data, https://files.consumerfinance.gov/f/2016_cfpb_privacy-impact-assessment-supervision-enforcement-and-fair-lending-data.pdf.

third-party PII with authorized external federal and state agencies to support the Bureau and other agencies' law enforcement activities.

In addition to whistleblower tip submissions, the CFPB receives tip information from other federal and state agencies. Tip information may be provided to keep the Bureau apprised of potential violations of federal consumer financial laws. Agencies, such as the United States Occupational Safety and Health Administration (OSHA), may provide information concerning employee claims of retaliation for reporting potential violations of the Bureau's statutes or rules.

Once the tip information is received by phone, mail, or email and a tip record is created within the WTD application, Enforcement intake staff process the tip. If contact information is provided, intake staff may follow up with the whistleblower. Any new information gathered by the intake staff will be stored in the tip record, along with any action taken on the tip. Records of subsequent actions, including investigative activities or actions initiated as a result of the tip, are not maintained within the WTD application.

Enforcement's intake staff also evaluate whether the tip contains potentially privileged information, such as communications between the company's attorney and the company, or written materials prepared by attorneys in anticipation of litigation. If potentially privileged information is identified, then the tip is routed to designated Enforcement staff with specific permissions within the WTD application to access the potentially privileged information for further review to determine whether it is privileged and should be redacted from the records.

The collection of whistleblower tip information, including PII, is authorized by sections 1012, 1021, and 1051 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. §§ 5491, 5492, 5511. The collection, maintenance, and use of the information is covered by CFPB.004 Enforcement Database system of records notice (SORN).[9] This SORN covers individuals who have inquired about or may have information concerning a possible violation of federal consumer financial law.

Furthermore, the WTD application resides within the CFPB Salesforce cloud platform and leverages the capabilities of the cloud architecture to support the secure collection of tips and automated tracking of actions related to the tip. The WTD application also inherits security and

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

privacy safeguards from the CFPB Salesforce platform including data storage, system computing resources (such as routers and firewalls inside data centers), software maintenance (such as security patches and secure upgrades), and access management tools. Limited information and PII about CFPB Staff[10] is captured when it is imported into the Salesforce cloud platform through the Bureau's identity management system for account generation and system access. The collection of this information is covered under the CFPB.014, Direct Registration and User Management System (DRUMS) SORN.[11]

Privacy Analysis and Risk Management

The CFPB conducts Privacy Impact Assessments (PIAs) on both programs and information technology systems pursuant to Section 208 of the E-Government Act of 2002[12] and in alignment with Office of Management and Budget (OMB) guidance and National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with the WTD application that support Enforcement's industry whistleblower program pursuant to the Fair Information Practice Principles (FIPPs). This includes the design and implementation of administrative, technical, or physical safeguards or controls, as applicable.

1. Characterization of Information

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

The WTD application maintains tip information that whistleblowers voluntarily submit by phone, mail, or email about entities and individuals under the CFPB's jurisdiction. Whistleblowers decide what tip information to share, including any PII such as name, job title, and contact information (*e.g.,* phone number, email address). The Bureau does not request or require specific information, data elements, or PII in whistleblower tip submissions. Tips may also contain other

[10] CFPB Staff means all employees, interns, volunteers, contractors, and details assigned to the CFPB.

[11] *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/.

[12] 44 U.S.C. § 3501 note.

information or PII about third parties associated with the entity or individual that is the subject of the tip.

While the CFPB collects and maintains all information submitted by the whistleblower in the WTD tip record, the Bureau primarily uses the whistleblowers' contact information, if provided, to follow up with the whistleblower to gather additional information, in support of enforcement and supervisory activities. Whistleblowers may opt to remain anonymous by not providing their PII when submitting their tip information to the Bureau, or by indicating that they would like to remain anonymous when providing their PII. Tip information is used, shared, and maintained as described within this PIA regardless of whether the whistleblower remains anonymous or provides PII.

Additionally, limited PII about CFPB Staff is accessible from the WTD because the application is integrated with the Bureau's identity management system for account generation and system access purposes. This information includes name, title, department, Bureau email, Bureau address, and Bureau phone number. Security of the PII within the WTD application is controlled through technical and administrative safeguards.

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

Whistleblowers may submit tip information directly to the CFPB via phone, mail, or email using the contact details listed on the Industry Whistleblower webpage of the CFPB's public website.[13] Additionally, the CFPB's Office of Consumer Response coordinates with Enforcement to share whistleblower tips erroneously received through their channels. Other federal agencies and state agencies may also share tips with the Bureau voluntarily. Tips from other federal or state agencies are submitted via email and are recorded within the WTD application as "outside agency".

For tips received by email, a tip record is automatically created within the WTD. For all other tips, Enforcement intake staff manually create a tip record in the WTD application.

- Email – The whistleblower can send an email to the designated Bureau email address, whistleblower@cfpb.gov, and it is routed to a secure email inbox. The WTD application

[13] See https://www.consumerfinance.gov/enforcement/information-industry-whistleblowers/

automatically creates a tip record and pulls in the email message content, including the email address and any attachments, for Enforcement intake staff review. The email is also attached to the tip record.

- Mail – The whistleblower can send a written communication to the designated mailing address on the Bureau's website. Upon receipt, an Enforcement intake staff member creates a tip record within the WTD application and attaches digital scans of the original documents to the tip record. The mailed correspondence is shredded after it is scanned and attached electronically to the tip record.
- Phone/Voicemail – The whistleblower can call the designated Bureau Whistleblower Tip line (855) 695-7974 to leave a voicemail message in the associated voicemail box. The CFPB employs transcription software to transcribe the voicemail message to text. An Enforcement intake staff member reviews the transcription for accuracy and attaches both the transcription and audio files to the WTD tip record.

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

The whistleblower tip information collected by the Bureau and maintained in the WTD application is not subject to the PRA requirements because the written and oral tip submissions do not ask "identical" questions of ten or more persons as defined in 5 C.F.R. 1320.3(c). Furthermore, any standardized follow-up questions would be excluded from PRA coverage as they would qualify as an "investigation" under 5 C.F.R. 1320.4.

1.4 Discuss how the accuracy of the information is ensured.

The whistleblower tip information in the WTD application is collected directly from whistleblowers. Tip submissions collected by email or mail are incorporated exactly as submitted. Voicemail tips are transcribed by software, and Enforcement intake staff review these transcriptions for accuracy before uploading them along with the audio files to the WTD application. Tip submissions provided by whistleblowers are accepted as accurately reflecting the whistleblower information as the information is collected directly from the whistleblower.

Only whistleblowers who identify themselves may contact the CFPB to have their information updated in the WTD. If Enforcement staff engage with a whistleblower to collect additional information about the substance of the tip, they also confirm the whistleblower's tip information.

If whistleblower tip information obtained from other agencies does not contain the whistleblower tip information collected directly from the whistleblower, Enforcement intake staff will seek to obtain it either from the agency or whistleblower directly.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that the CFPB may use the information collected within the WTD for a purpose other than for which the information is collected.

Mitigation: This risk is mitigated through the established process of submitting tips to the CFPB. Whistleblowers submit information directly to the CFPB via phone call and/or voicemail, mail, or email. Additionally, the Bureau's Office of Consumer Response coordinates with Enforcement to share whistleblower tips erroneously received through their channels. Other agencies also share tips with the Bureau. The whistleblower may opt to remain anonymous by not providing their PII when submitting their tip to the Bureau, or by indicating that they would like to remain anonymous when they do provide PII. Tip information, including PII, may be shared with external federal and state entities for the pursuit of investigations as deemed appropriate by the Bureau, and in accordance with the routine uses published in the applicable SORNs, 12 C.F.R. part 1070, and other applicable laws. Sharing of any whistleblower information, including PII, is strictly managed through memoranda of understanding (MOU) and/or via approved access request, and access is provided consistent with relevant statutes, regulations, and case law.

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).

The purpose of Enforcement's industry whistleblower program is to identify potential industry misconduct. Although CFPB does not require specific PII in whistleblower tip submissions, all information submitted voluntarily, including PII, is collected and maintained in the WTD. If submitted, the CFPB may use the PII to contact the whistleblower for additional details, to clarify tip information, or to support its enforcement or supervisory activities.

Enforcement staff members with access to the WTD must be trained to handle whistleblower information and follow strict whistleblower guidelines and policies governing the use of that information, including PII. Additionally, the Bureau implements access controls within the WTD application, such as single sign-on (SSO), to enforce need-to-know principles. Only Enforcement staff who support the operation or maintenance of the WTD, and who otherwise have job responsibilities in Enforcement that require access to information in the WTD, are authorized by the system/product owners to access the WTD application and to view tip record information.

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.

The whistleblower tip records collected and maintained in the WTD application are retained in accordance with the National Archives and Records Administration (NARA) approved CFPB records disposition schedule N1-587-12-008, item 1, and by reference in items 2-5.

The items identify different retention schedules depending on Enforcement's use of and need for the information. Generally, the disposition of these records is temporary and are destroyed or deleted six months after the cutoff. However, if the record is being used for a specific matter in items 2-5, then it becomes a matter record and is subject to the disposition schedule as it applies to the item, which can range from 1 to 15 years beyond the year created to permanently archived for historically significant cases.

Records used to grant Enforcement staff access to the WTD application as described within the Direct Registration and User Management System (DRUMS) system of records notice are retained in accordance with General Records Schedule (GRS) 3.2, Item 031 and are destroyed 6 years after password is altered or user account is terminated.

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

Privacy Risk: There is a risk that the whistleblower may provide more than the necessary amount of PII needed for the Bureau to contact them or investigate the tip.

Mitigation: While the CFPB collects and maintains all submitted information, Enforcement primarily uses the contact information to contact whistleblowers if additional information regarding the tip is needed. Any whistleblower tip information provided to Supervision is redacted to exclude the whistleblower's PII. External federal and state agencies supporting the Bureau and other agencies' law enforcement activities may need PII, but generally, only the tip details, and not the whistleblower's PII, are shared with those agencies. The Bureau also minimizes data collection by not accepting privileged information, including confidential communications between the company's attorney and the company, or written materials prepared by attorneys in anticipation of litigation. If privileged information is submitted with the tip, Enforcement intake staff identifies it as such and either redacts the information before routing it for further review or segregates the tip from further access or review. Additionally, in the exceedingly rare instances when Social Security numbers (SSNs) are provided and the tip is potentially actionable, then Enforcement intake staff redact the information before routing the tip for further access or review.

3. Uses of Information

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

The CFPB uses tip information to support the Bureau's enforcement and supervisory activities that include investigation and examination of covered persons or service providers' practices for potential violations of federal consumer financial law. To that end, Enforcement may share tip information with identifying information redacted, with the Supervision Division (Supervision). The whistleblower tip information may include the whistleblower's PII and the tip details (*e.g.*, conduct that may potentially violate any federal consumer financial laws, PII of third parties). The whistleblower's contact information, if provided along with the tip, may be used by Enforcement staff to follow up with the whistleblower. Moreover, Enforcement uses the tip details to determine whether the tip supports an existing investigation or warrants a new investigation.

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

Enforcement may share whistleblower tip information with the Legal Division when the tip, for example, may be subject to disclosure through a legal discovery process or at trial. It may also share the tip details with Supervision for potential action related to the CFPB's supervisory responsibilities; however, it does not generally share PII with Supervision.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There are risks that the information may be misused or used for unauthorized purposes.

Mitigation: The CFPB mitigates these risks by limiting access to whistleblower information to trained Enforcement staff whose job responsibilities give them a need to access the WTD and handle whistleblower information. Strict whistleblower guidelines and policies governing the use of this information and access controls within the WTD application help enforce need-to-know principles. Only Enforcement staff who support the operation or maintenance of the WTD, and who otherwise have job responsibilities in Enforcement that require access to information in the

WTD, are authorized by the system/product owner to access the WTD application and view tip information.

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.

The publication of this PIA and the CFPB.004 Enforcement Database SORN provide general notice to the public on the intended purpose and use of PII that is voluntarily submitted as part of tip information. Furthermore, the CFPB's Industry Whistleblower public webpage provides a Privacy Act Statement outlining how information will or may be shared, and the recorded greeting and introduction message on the whistleblower tip line provide information about how to submit a tip to the Bureau.[14]

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.

Submission of a tip is entirely voluntary; by submitting the tip the whistleblower is consenting to its use by the CFPB as described on the CFPB's Privacy Act Statement, which is linked to from the Industry Whistleblower webpage. CFPB may use any information submitted by an individual. If a submitter raises concerns through the tip submission about the use or sharing of information provided within a tip, Enforcement staff will reach out to the submitter, if possible, to explain the scope of confidentiality of their information.

In addition, the webpage describes protections against retaliation and discrimination for 'covered employees' under 12 U.S.C. § 5567, as well as for employees who report unsafe or unhealthful conditions or exercise rights through OSHA. The outgoing message for whistleblowers who telephone and leave voicemail messages also affords callers the opportunity to learn more about their protections.

[14] Please see https://www.consumerfinance.gov/enforcement/information-industry-whistleblowers/ for more information.

Third-party individuals who may be named in a whistleblower tip do not have the ability to consent to the use of their information or to obtain redress. To mitigate this risk, Enforcement staff only share reasonably creditable PII with federal and state regulators.

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

Individuals may request access, amendment, or correction to their records maintained in the WTD application by contacting 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, promulgated at 12 C.F.R. 1070.50 *et seq*.[15] The access, notification, and contesting procedures are also available through the CFPB.004 Enforcement Database SORN. Individuals who have any questions may contact the CFPB FOIA Office via FOIA@CFPB.gov or at (855) 444-3642. Some records, such as those related to a CFPB enforcement investigation or action, may not be subject to access or amendment. Additional information can be found on CFPB's Privacy website.[16]

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that the whistleblower does not fully understand how their information may be used once the tip is submitted to the CFPB.

Mitigation: Tip information is voluntarily submitted to the Bureau. Whistleblowers can choose to submit the tip to the Bureau without providing their PII, although sending the tip by personal email might necessarily cause limited PII (*i.e.*, email address) to be collected. The CFPB's Industry Whistleblowers public webpage provides information regarding submission of tips via phone and voicemail, email, or mail correspondence. The webpage also provides notice that whistleblowers are not required to submit any PII and advises how collected information, including PII, is used. Whistleblower tips received by the Office of Consumer Response and shared with the Enforcement Division may also include PII. If PII about a third-party is included within the tip information, that individual is not provided with notice or consent.

5. External Sharing and Disclosure of Information

---

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

[16] Please see https://www.consumerfinance.gov/privacy/.

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.

Tip information, including PII, may be used in accordance with the routine uses published in the CFPB.004 Enforcement Database SORN.

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

Sharing of any whistleblower information with third parties, including PII, is strictly managed through memoranda of understanding (MOU) and/or via approved access requests, and access is provided consistent with relevant statutes, regulations, and case law.

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

Privacy Risk: Given the content and sensitivity of information held within the WTD, the WTD application may be a target for unauthorized access and/or be at risk for insider threats.

Mitigation: Information within the WTD is 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), Risk Assessment (RA), and Systems and Communications Protection (SC) controls, are implemented to restrict access to the information to only authorized Enforcement staff.

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

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 of 1974,[17] the Right to Financial Privacy Act,[18] and Section 208 of the E- Government Act of 2002.[19] To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopts the FIPPs, the framework for its privacy policy.[20] 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 also adheres to the Office of Management and Budget privacy-related guidance[21] as a best practice, and applies the NIST Risk Management Framework (RMF)[22] for information technology systems, applications, solutions, and services. The CFPB identifies and applies NIST SP-800-53[23] security and privacy controls and continuous monitoring of controls to ensure on-going compliance with information security standards and protect organizational operations and assets and individuals. The WTD application is developed using the agile methodology. As such, system change requests and security assessment and authorization (SA&A) documentation address privacy relative to systems development, including, as warranted and appropriate: statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment.

[17] 5 U.S.C.§ 552a

[18] 12 U.S.C. §§ 3401-3423.

[19] 44 U.S.C. § 101.

[20] *See* CFPB PRIVACY POLICY (Dec. 6, 2012), and subsequent updates.

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

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

[23] *See* NIST Security and Privacy Controls for Information Systems and Organizations, SP-800-53, Rev. 5 (September 2020), as updated in Release 5.2.0 (August 2025). For more information visit https://www.nist.gov.

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

All CFPB Staff are required to adhere to all CFPB cybersecurity and privacy policies and take mandatory annual training. For example, Enforcement staff are required to take the CFPB Privacy Training, the Cybersecurity Awareness Training, and the Privileged User Training within thirty days 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. The 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?

The CFPB employs and uses role-based access controls to ensure CFPB Staff, including Enforcement staff, have access to only the system and/or information necessary and relevant to their assigned duties. Only Enforcement staff who have assigned duties relevant to the whistleblower program have access to the WTD. CFPB Staff responsible for providing technical support for the WTD application have access to the WTD. No other systems or individuals have access to the data used by the Enforcement's industry whistleblower program. Enforcement is responsible for assigning and maintaining roles and permissions within the program and its applications based on an individual's role within the organization and as approved by CFPB Cybersecurity.

CFPB Staff with access to CFPB information and systems and facilities are required to proceed through background investigations for suitability and security clearance determinations. 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.

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

Privacy Risk: Given the content and sensitivity of the information held within the system, the data may be a target for unauthorized access and/or be at risk for insider threats.

Mitigation: The CFPB mitigates these risks in several ways. First, information is protected through robust security controls, both physical and technical, within the particular environment where it is housed, and the use of secure network protocols for transmission of data outside of the environment (or between environments). The CFPB has implemented technical controls to prevent and detect unauthorized access or changes to systems, computer programs, and information. Moreover, the CFPB limits access to information on projects to authorized individuals using the concept of least privilege and on a need-to-know basis only. In general, Enforcement staff is assigned a unique authentication ID for access to systems. CFPB Staff information security policies exist for security administration, monitoring, and information security. Access to any PII and other sensitive information is restricted and must be approved by Enforcement's industry whistleblower program lead.

Document control

Approval

Christopher Chilbert

Chief Information Officer

Date

Kathryn Fong

Chief Privacy Officer

Date

Danny Pham

System Owner

Date

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

Change Control

Version	Summary of material changes	Pages affected	Date of change
1	Original Approval		December 2020
2	Updated to address the use of voicemail transcription software; revise name of program office; transfer into a newer template; general updates.	All	August 2026