Enforcement Whistleblower Tip Database Application PIA v.1

Does the CFPB use the information to benefit or make a determination about an individual?	No
What is the purpose?	To collect, track, and analyze whistleblower tips and contact information concerning companies or individuals for potential violations.
Are there controls to enforce accountability?	Yes. All standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Appropriate opportunities for notice, consent, access, and redress.

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Act"), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau ("CFPB" or "Bureau"). The Bureau administers, enforces, and implements federal consumer financial protection laws. In carrying out its responsibilities, the Bureau is involved in the collection of whistleblower tips and information from the public about possible misconduct committed by companies or individuals and is empowered by the Act to investigate potential violations of federal consumer financial law. The Act also includes whistleblower protections for individuals who report information about potential violations of the law.[1]

The Bureau's Supervision, Enforcement & Fair Lending (SEFL) Division, Office of Enforcement collects whistleblower tip data related to potential violations of law, including:

- Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act (CFPA);
- Any other provision of law subject to Bureau jurisdiction; and
- Any rule, order, standard, or prohibition prescribed by the Bureau.

To facilitate the collection of this information, the Office of Enforcement created the Whistleblower Tip Database (WTD) application to electronically collect tips voluntarily submitted by whistleblowers, and to create records of the tips for processing by the Bureau in an efficient and accurate manner. Whistleblowers, including industry insiders and current or former employees of financial institutions, may alert the Bureau to potential violations of federal consumer financial laws. The WTD application allows the Bureau to consolidate, track, task, and manage the whistleblower tip records, and create real-time, ad hoc, or on-demand reports to determine whether there are potential violations.

When providing the tip information, the whistleblowers may choose to include personally identifiable information (PII) with their submission, such as name, job title, and contact information. Whistleblowers determine what information they want to share with the Bureau, to include their PII; the whistleblower can submit a tip without providing PII, and the Bureau does not request specific data elements or PII be included in whistleblower tip submissions. If name and contact information

[1] *See 12* U.S.C. § 5567.

are submitted with the tip, the Bureau may use the information to contact the individual for more information to help facilitate its analysis of the tip and the potential investigative process.

While the Bureau includes all information that a whistleblower chooses to provide into the tip record, the Bureau uses whistleblower PII to contact whistleblowers for additional information. The PII may also be used to support the Bureau's enforcement and supervisory activities that include investigation and examination of potential violations of federal consumer financial law. In support of these activities, PII may be shared by the Office of Enforcement with the Office of Supervision (also within SEFL) to examine financial services company practices, support investigative processes, and ensure compliance with financial law.[2] Tip information may also include PII pertaining to a third-party individual affiliated with the company or financial entity that is the subject of the tip. Third-party PII submitted as part of the whistleblower tip 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. PII submitted with a tip may also be shared with external federal and state agencies to support the Bureau and other agencies' law enforcement activities.

Whistleblowers have the option to submit tips confidentially. If a whistleblower requests confidentiality when submitting a tip, the Bureau endeavors to keep the identity private, including PII. When confidentiality is requested, the record is clearly flagged so that any subsequent Office of Enforcement user understands this preference and handles the record consistent with relevant statutes, regulations, and case law. However, if the information is used in litigation, then PII submitted with the tip may be disclosed, as the identity of the whistleblower and the content of the tip may be part of litigation and subject to disclosure through the discovery process or during trial proceedings. The Office of Enforcement collects whistleblower tips, to include PII voluntarily submitted by whistleblowers, through four methods:[3]

- Email – the whistleblower can share information by sending an email to the designated Bureau email address, whistleblower@cfpb.gov. The email submission may include the

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

[3] For more information on submitting whistleblower tips and whistleblower protections, see the CFPB Office of Enforcement's public website, https://www.consumerfinance.gov/policy-compliance/enforcement/information-industry-whistleblowers/.

whistleblower's PII, such as his or her email address and first and last name. WTD has the capability to automatically pull relevant email message content into a tip record template for Office of Enforcement staff review, to include the individuals email address.

- Mail – the whistleblower can send a written communication to the Bureau to the designated mailing address and point of contact indicated on the Bureau's website. Upon receipt, Bureau staff creates a tip record within WTD. The team also scans the original documents and attaches electronic copies of the correspondence to the tip record. Whistleblowers may provide PII, such as first and last name and mailing address, or they may choose to remain anonymous. The mailed correspondence is stored in locked files after it is scanned and attached electronically to the tip record.
- Phone - the whistleblower can call the designated Bureau hotline to leave a voicemail on the tip line. Office of Enforcement staff checks this voicemail daily and inputs the tip information from the voicemail into the WTD. The voicemail is deleted after the tip information is entered into the WTD.
- The Bureau's Consumer Response Office may receive whistleblower tips that are erroneously submitted to it. Consumer Response coordinates with the Office of Enforcement to share misdirected tips, including any PII received. Bureau staff then enter whistleblower information into the WTD.

The Bureau also receives tip information from other agencies, such as the United States Occupational Safety and Health Administration (OSHA). OSHA provides information concerning employee claims of retaliation for reporting violations of the Bureau's statutes or rules. Tip information may be provided to the Bureau to keep the Bureau apprised of potential violations of consumer protection laws.

Once the tip is received and the tip record is created within the WTD, Office of Enforcement Intake staff review the information. If PII is provided within the tip record, Intake staff may follow up with the whistleblower for additional information about the tip. Intake and other Office of Enforcement staff reviewing tip information 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, the information is flagged and reviewed by other Office of Enforcement staff to determine whether it is privileged and should be redacted from the records.

The Office of Enforcement does not use PII for any purposes other than those identified in this PIA. Any records of investigations initiated as a result of the tip are maintained in a separate system.

The collection of whistleblowers' PII is authorized by Public Law 111-203, Title X, sections 1012, 1021, and 1051 *et seq*. codified at 12 U.S.C. 5491, 5492, 5511 *et seq*. The collection, maintenance, and use of the information are covered by *CFPB.004 Enforcement Database*.[4] This SORN covers individuals who have inquired about or may have information concerning a possible violation of federal consumer financial law.

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.

The Paperwork Reduction Act (PRA) does not apply to the WTD. The written submission of whistleblower tips is made through email or free text; the WTD does not ask "identical" questions of ten or more persons as defined in 5 CFR 1320.3(c). Furthermore, any standardized follow-up questions would be excluded from PRA coverage as it would qualify as an "investigation" under 5 CFR 1320.4.

Privacy Risk Analysis

The WTD application may collect PII from individuals who voluntarily submit it. Information provided by a whistleblower may also include PII about third parties, such as individuals at a company that the whistleblower works or worked for, individuals who may be in violation of consumer financial laws, or information about another company. The inclusion of PII in a whistleblower tip record significantly raises the sensitivity of the data and associated privacy risks. The whistleblower or other individuals associated with the tip may face embarrassment, exposure, or scrutiny from an employer or colleagues if their information is breached or disclosed to unauthorized users. Accordingly, this PIA examines these risks and measures that the Bureau implements to mitigate those risks. The Bureau's Privacy Program has considered system privacy controls that mitigate primary risks associated with the WTD application related to the following privacy principles:

- Limits on Uses and Sharing of Information
- Data Minimization

[4] A complete list of CFPB SORNs can be found here: https://www.consumerfinance.gov/privacy/system-records-notices/.

- Individual Participation
- Security

Limits on Uses and Sharing of Information

There are risks that the information may be misused or used for unauthorized purposes. The Bureau mitigates these risks by only using PII to contact the whistleblower for additional details to clarify tip information and to support its enforcement and supervisory activities. Any staff member with access to PII from the WTD must be trained to handle whistleblower information and follow strict whistleblower guidelines and policies governing the use of that information. Additionally, the Bureau implements access controls within the WTD that enforce need-to-know principles. Only internal Office of Enforcement staff members supporting operation and maintenance of the WTD are authorized by the system/product owner to access the application and view tip record information. Furthermore, any disclosure of tip information to external entities must be done in accordance with the routine uses published in the applicable SORN, and as authorized under applicable laws.

Data Minimization

The Bureau collects PII through the voluntary submission of tips and information related to the tip. The Bureau does not require or request specific data elements or PII in a tip submission; however, there is a risk that the whistleblower may provide more than the necessary amount of PII needed for the Bureau to investigate the tip. While the Bureau includes all information submitted by the whistleblower into the tip record, the Bureau only uses the PII provided to contact whistleblowers for additional information and to support the Bureau's enforcement activities that include investigation of potential violations of federal consumer financial law. It may be used by the Bureau's Office of Supervision to support its supervisory work as well. The PII may also be shared with external federal and state agencies to support the Bureau and other agencies' law enforcement activities.

Additionally, the Bureau does not accept 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, the Office of Enforcement 's staff identifies it as such and either redacts the information before routing it for further review or segregates the tip from further review.

Individual Participation

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 Office of Enforcement's Information for

Industry Whistleblowers public website provides information regarding submission of tips via phone, email, or mail correspondence. The website 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 Consumer Response and available to the Office of Enforcement 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.

Security

Given the content and sensitivity of information held within the WTD, the database may be a target for unauthorized access and/or risk insider threats. Information within the WTD will be 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), Risk Assessment (RA), and Systems and Communications Protection (SC) controls, will be implemented to restrict access to the information to only authorized Office of Enforcement staff.

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

Privacy Risk Management

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

The WTD application is used to collect tip information voluntarily submitted by whistleblowers against financial entities or companies or individuals at companies. As part of the submission process, whistleblowers may submit their PII with tip information to include their name, job title, and contact information. The whistleblower tip may also contain other information or PII related to third parties associated with the financial entity or company that is the subject of the tip. Whistleblowers determine what information they want to share with the Bureau, to include their PII. The Bureau does not request or require that specific data elements or PII be included in whistleblower tip submissions. While the Bureau includes all information submitted by the whistleblower into the tip record, the Bureau only uses the PII provided to contact whistleblowers for additional information and to support its enforcement and supervisory activities.

The whistleblower can submit information directly to the Bureau via phone call, physical mail, or email into a secure email inbox. Additionally, the Bureau's Consumer Response Office coordinates with the Office of Enforcement to share whistleblower tips erroneously received through their channels. Other agencies, such as OSHA, also share tips with the Bureau. Once the Office of Enforcement receives the submitted tip, Intake staff members enter the information into the WTD application and create a tip record. 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 the Bureau to keep their identity confidential.

Additionally, some information about employees and contractors working for the Bureau is captured when it is imported into the WTD application through 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.

2. Describe CFPB's objective for the information.

The WTD application manages whistleblower tip information, including details related to the tip, any PII included with the tip, and the information on the financial entity or company referenced in the tip. The Bureau uses the information maintained in the WTD to determine whether the tip supports an existing investigation, or if a new investigation should be initiated based on the tip. The information captured in the tip and maintained in the WTD supports the Bureau's investigation of the tip as a potential violation of federal law. PII, if provided along with the tip, is only used by the Bureau for the purpose of following up with the whistleblower and to support its enforcement and supervisory activities. Information pertaining to authorized Office of Enforcement employees and contractors accessing the WTD is collected and maintained by the system to allow a user to log in, conduct an internal review of the responses, and flag responses that include specific criteria highlighted by the Bureau. Outside of these uses, PII is not used for any other purposes.

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

The Office of Enforcement shares tip information, including PII, with other federal and state regulators under certain circumstances if the Bureau determines that it likely falls under the agency's jurisdiction. The Bureau shares information consistent with relevant legal requirements. As in all instances, upon whistleblower request, the Bureau endeavors to keep information shared by whistleblowers confidential, including their PII. However, if the information is used in litigation, then it could be disclosed, and the identity of the whistleblower and the content of the tip may be subject to

disclosure through the discovery process or at trial. The use and sharing of the tip information are consistent with the routine uses published in the *CFPB.004 Enforcement Database SORN*. Any disclosures by the Bureau are subject to the Bureau's regulations at 12 CFR part 1070.

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.

The publication of this PIA and the *CFPB.004 Enforcement Database SORN* provide notice to the public on the intended purpose and use of PII that is voluntarily submitted as part of tip information. Furthermore, the Office of Enforcement's Information for Industry Whistleblower public website and outgoing message on the whistleblower hotline provide additional notice on how to submit a tip to the Bureau. The whistleblower consents to the Bureau's use of the information when he or she voluntarily submits it. The website also describes whistleblower protections and rights afforded to whistleblowers through OSHA. Furthermore, the website provides information on how to submit a complaint to OSHA if whistleblowers suspect they have been fired or retaliated against for reporting violations against their employer. The Bureau gives individuals the ability to request access and amendment to 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*.

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 address this risk the Office of Enforcement staff only shares this PII with federal and state regulators when there is a likely violation of the law.

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

A full security review of the Platform hosting the WTD application has been conducted by the Bureau based on all applicable federal laws, directives, and standards. The Bureau has developed and followed a Security Implementation Plan (SIP) identifying the necessary steps to store PII within the Platform. Additionally, the Bureau Platform and WTD application will receive an Authority to Operate (ATO) in accordance with Bureau policies and National Institute of Standards and Technology (NIST) guidance.

The Bureau issues authorized personnel access to the platform following the Bureau's User Access Request process. Some users may also include authorized Bureau contractors. Employees and contractors must complete system training, including confidentiality and privacy briefings, prior to

being granted access to the application. Users will be granted roles based on their division and need to access the data in the system. Because whistleblowers may submit PII when they voluntarily submit their tips, the Bureau uses the following technical and administrative controls to secure the data and create accountability for the Bureau's appropriate collection, use, disclosure, and retention of the information:

- Implementation of applicable 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: Initial access to data are established as private within the application, meaning only the data owner can see the data; but with the Application Owner's approval, additional data sharing rules may be built into the system that may allow multiple users to see data on a divisional or organizational wide basis. The following internal users will have access to information collected and maintained by the WTD application:
    - Office of Enforcement staff members (Internal Bureau Users): Internal users (Enforcement full time employees and contractors) will have access to WTD application, which will grant them access to the whistleblower tip, entity, and person account data within the application, but their access will be limited based on system built security model.
    - Developers (Internal Bureau Users): Developers have administrator access in the sandbox (i.e., testing) environments they work in. Developers have access to User Acceptance Testing (UAT) sandboxes that contain a full copy of production data from the WTD application to allow for full testing of the applications. Developers do not have access to the production environment and cannot make changes to the system without support of the release management team. Requests must be submitted for elevated access.
    - Business Analysts (Internal Bureau Users): Business Analysts work with development teams to configure the WTD application and have Administrator level access in both the team development sandboxes and the UAT sandboxes to assist with development and testing of the applications. Business Analysts do not have access to the production environments and cannot make changes to the system without support of the release

management team. Requests must be submitted for elevated access. Business analysts do not have regular access to PII maintained within the WTD. Business analysts do, for a time, have access to the PII when conducting data transfer from legacy systems to the WTD. Once the initial data transfer is complete and the data goes live in the production environment, a business analyst no longer has access to that data and will not have access to that data moving forward.

  - Release Management Team (Internal Bureau Users): The Release Management Team has Administrator level access in all environments including the WTD application production environment to conduct deployments and make system changes as necessary.

  - System Administrators (Internal Bureau Users): Platform system administrators have full access to the system, data, and all applications within. System administrators are considered privileged users and as such will have access to all data in the system, including PII associated with a tip record, for the purposes of controlling, monitoring, and other administrative functions. These system administrators have elevated access within the production and lower environments, which have been approved by the platform owner, as well as the Information Security owner.

- Personnel Security, including background checks of contractors and federal employees.
- Records Retention Requirements: The Bureau maintains the whistleblower tip information in accordance with the National Archives and Records Administration (NARA) approved schedule. The records are covered in item 1 of the NARA approved Records Disposition Authority for Enforcement. The disposition of whistleblower records is temporary and are destroyed or deleted six months after the end of the calendar year when the record is created. The longest retention period would total 18 months, if the information is no longer needed to support a Bureau activity. If the whistleblower 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.

As a result of conducting this PIA, the Bureau is revising the Privacy Act Statement and the Enforcement website to ensure its clarity and accuracy.

6. Discuss the role of third party(ies) that collaborate or partner with the Bureau, 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 Bureau, e.g., government contractors discussed in Question 5.)

Tip information, to include 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 CFR part 1070, and other applicable laws. Sharing of any whistleblower information, to include 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.

Document control

Approval

Christopher Chilbert

Digitally signed by Christopher Chilbert
Date: 2020.12.15 11:24:20 -05'00'

Christopher Chilbert

Chief Information Officer

TANNAZ HADDADI

Digitally signed by TANNAZ HADDADI
Date: 2020.12.15 11:53:33 -05'00'

Tannaz Haddadi

Chief Privacy Officer

Rebecca Gelfond

Digitally signed by Rebecca Gelfond
Date: 2020.12.11 19:02:31 -05'00'

Rebecca Gelfond

Initiative Owner

Change control

Version	Summary of material changes	Pages affected	Date of change
1	New Publication	All	