Civil Penalty Fund and Bureau-Administered Redress Program v.3

Privacy Impact Assessment

November 2024

Consumer Financial Protection Bureau

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). 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. In executing its duties, the CFPB collects information to successfully administer the Civil Penalty Fund and Bureau Administered Redress Program (interchangeably referred to as "the Civil Penalty Fund and Redress Program" or "the program" hereafter).[1] The CFPB's Chief Financial Officer is responsible for administering the program[2].

When a person or company violates a federal consumer financial protection law, the CFPB can bring an enforcement proceeding against them. If that person or company is found to have violated the law, it may be required to pay a civil penalty, also known as a civil money penalty (CMP). The CFPB collects and deposits the CMPs into its Civil Penalty Fund[3] and primarily uses these funds to financially compensate eligible victims[4] harmed by illegal actions for which CMPs have been imposed. The CFPB may also obtain other types of monetary relief, or redress, through judicial and administrative proceedings that the CFPB uses to make payments to victims harmed by a company or person's activities. This is called Bureau-administered Redress.

For all matters resulting in redress or Civil Penalty Fund payments, the CFPB is responsible for monitoring the distribution of funds held in the Civil Penalty Fund or in an account designated for Bureau- administered Redress to victims. The CFPB either directly manages the distribution of funds to harmed victims or issues contractual task orders specific to a matter to a contractor working on behalf of CFPB to provide some (or all) of the following services:

---

1 Read more about the Civil Penalty Fund at https://www.consumerfinance.gov/about-us/payments-harmed-consumers/civil-penalty-fund and https://www.consumerfinance.gov/enforcement/payments-harmed-consumers/payments-by-case/.

2 The Civil Penalty Fund Administrator is responsible for administering payments from the Civil Penalty Fund, but reports to, and is removable by, the Chief Financial Officer. 12 C.F.R. § 1075.102(a).

3 *See* 12 U.S.C. § 5497(d).

4 *See* 12 C.F.R.§§ 1075.101 ('Victim'), 1075.103 (Eligible Victims).

- Funds management – Contractors must manage specified funds related to a particular matter, including establishing an account (to hold the funds) and reporting.
- Communication and help services for consumers and the public – For each assigned matter, the contractor is the primary public contact for fund distribution activities. The contractor prepares public communications as described in the matter- specific task order. The contractor's responsibilities include responding to public inquiries and addressing harmed victims' specific complaints or disputes.
- Claims processing – Contractors manage the collection and verification of claims-related documentation for matters requiring a claims process after the eligible victims have identified or verified themselves as a harmed eligible victim and request payment from CFPB's Civil Penalty Fund and Bureau-administered Redress Program.
- Fund distribution – The assigned contractor distributes funds from the established account to eligible victims as directed by the CFPB through the specific task order. Each matter requires the maintenance of a specific system(s) tracking contact information and payment information. Additionally, sometimes the contractor is required to timely and cost-effectively locate harmed victims contact information.
- Reporting – For each assigned matter-specific task order, the contractor is required to provide the CFPB with monthly and ad hoc reports on activities, including funds distribution, tracking, and public communication. Additionally, the contractor may be required to provide tracking to evaluate the effectiveness of payment methods (*e.g.*, check, direct-deposit, pre-loaded debit cards) to support future program improvements, and as necessary, may need to produce reports for federal, state, and local taxing officials to help meet tax-reporting obligations.

The CFPB contractors may process and store, as necessary, information including personally identifiable information (PII) they receive either from the CFPB, directly from harmed victims, or from third parties. The Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111-203, Title X, Sections 1017(d) (Civil Penalty Fund) and 1055(a) (Redress), codified at 12 U.S.C. §§ 5497(d), 5565(a), allow the collection of this PII, including Social Security number (SSN) to administer the program. The PII is stored in matter-specific databases or systems in secure on-site and off-site locations.

The systems created and used by contractors vary based on the nature of the matter, but in general, contractors collect and maintain information such as:

- Database(s) of potential and eligible victims, their contact information, contact information about third parties who represent their interests, their potential and actual compensation amounts, successful and unsuccessful payment distributions, and any other relevant information for each matter;
- Potential harmed victims who inform the contractor, in writing, of their desire not to participate in the fund distribution;
- Potential harmed victims whose notification letters are undeliverable and potential harmed victims whose notification letters remain undeliverable even after attempts to obtain the corrected name and address information;
- Potential harmed victims who do not respond to the notification letter within the period specified for filing claims;
- Duplicate entries and consumers not eligible to receive a payment from a distribution;
- Potential harmed victims whose claim forms remain insufficient;
- All claims and supporting documentation submitted;
- Method and purpose of inquiries received from harmed victims;
- Number of unique visits to the matter or claim on the contractor's website if one is developed; and
- Number and details of address changes submitted and updated.

The original Privacy Impact Assessment (PIA) for the Civil Fund and Bureau-Administered Redress Program was published in August 2013 and last updated in December 2023. The CFPB is now updating this PIA in a new template to discuss the privacy risks and mitigations associated with the collection and use of new PII of third parties who represent the interest of eligible victims. It also documents the new collection of information related to benefits or need-based assistance to that helps CFPB further advise impacted victims on their compensation. The scope of this PIA is limited to the privacy risks and technical controls associated with the administration of the Civil Penalty Fund and Redress Program. This PIA does not cover any investigations or enforcement activities leading to the imposition of a CMP or redress. Any PII or information collected to support those preceding activities to payment are covered under separate PIAs. The program's information and records, except information about third parties who represent the interest of eligible victims are covered by the CFPB's system of records notice (SORN), CFPB.025, Civil

Penalty Fund and Bureau-Administered Redress Program Records.[5] This SORN gives notice of the information maintained and processed in the system.

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 2086 and in alignment with Office of Management and Budget[7] (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with the Civil Penalty Fund and Redress Program 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

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

The PII of eligible victims collected, used, disseminated, or maintained either by CFPB or within the contractors' systems varies depending upon the matter, but in general, includes:

- Name;
- Address;
- Transaction or claim information including:
  - Transaction dates;

[5] *See* CFPB.025 Civil Penalty Fund and Bureau-Administered Redress Program Records, 78 Fed. Reg. 34991 (Jun 11, 2013) and subsequent update 83 Fed. Reg. 23435 (Jun. 21, 2018), *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/civil-penalty-fund-and-bureau-administered-redress-program-records/.

[6] 44 U.S.C. § 3501 note.

[7] 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.

  - Company selling product and product type;
  - Customer number or account number; and/or
  - Harm amount.
- Internal identification number assigned to identified harmed victim;
- Email address; and
- Phone number and/or other contact information.

Additional information may be gathered to assist with processing claims and distributing funds for specific matters. These may include:

- Name and contact information of third parties who represent the interests of impacted victims or to whom the CFPB or its contractors is authorized to communicate with *e.g.,* legal guardians, power of attorney (POA) holders or agents. This information is not retrieved by a unique identifier;
- Name and contact information of individuals who help harmed victims fill out civil penalty or redress matter forms;
- Benefits or assistance information (including that of household members) to determine whether civil penalty and redress payouts could impact harmed victims' eligibility for some need-based government benefits.

Furthermore, in some cases, more sensitive PII may be necessary in some cases to facilitate and track the payment to eligible victims or to meet other reporting obligations, such as tax-reporting obligations. These may include:

- Social Security number or tax identification number;
- Date of birth (DOB);
- Marital status;
- Credit card numbers and card issuer names; and/or
- Bank account numbers and bank names.

The PII about other individuals with information relevant to a CFPB action that has resulted in an order to pay CMPs or redress to CFPB, may include the following information about employees and other individuals associated with entities or defendants:

- First and last name;
- Position or title;
- Work address;
- Home and work phone number; and
- Email addresses.

The PII described above is the minimum amount necessary to appropriately manage and administer CFPB's Civil Penalty and Bureau-administered Redress Program.

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

The PII of harmed victims may initially be collected or identified as part of an enforcement action or investigation. When eligibility for redress or compensation is determined, the program directly collects information from victims, defendants, third parties who represent the interest of eligible victims, or other third-party data sources.[8] The victims may also provide information directly to the Bureau through a consumer complaint filed with CFPB. CFPB collects such PII through a variety of methods. For example, some matters require a contractor to collect information directly from victims to make payment using a form (either physical or an electronic web form). For other matters, CFPB contractors receive information from third-party data sources. However, this is generally limited to address and other contact information corrections to facilitate identification or verification of, and payment to, victims.

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

OMB has approved the information collection regarding select claims (e.g., satisfaction surveys, Collection of Qualitative Feedback on Bureau Service Delivery) and assigned the information collection number OMB Control No. 3170-0024.

1.4 Discuss how the accuracy of the information is ensured.

[8] Third-party data sources may include public-record sources such as the United States Postal Service's (USPS) National Change of Address Database (NCOA) or LexisNexis (for address corrections, etc.).

In general, PII collected for the program is verified for accuracy, completeness, and timeliness in accordance with its original source or the technology originally used to collect it. In many instances, the CFPB or a contractor uses PII obtained about victims from defendants' files to mail payment directly to those victims. In other cases, claim forms are mailed to a known set of potential victims requesting that they validate information, including their address, harm amount (amount lost due to a defendant's violation of the law), and eligibility for payment. In still other cases, contractors make claim forms available to previously unknown eligible victims via a case-specific outreach effort, such as a dedicated website and web form. Harmed victims provide information including their address, harm amount, and eligibility for payment directly to the CFPB.

The contractor managing the matter is responsible for reviewing all payment distributions and claim form responses to confirm that the claims (including stated harm amount) are consistent with a set of established matter-specific parameters. Outreach material, checks, and claim forms always include a telephone number and email address for harmed victims to contact the contractor or CFPB to answer their questions or update their information. Furthermore, prior to a contractor mailing a claim form, check, or educational material, harmed victims addresses are standardized and validated against known data sources, such as the United States Postal Service National Change of Address (USPS NCOA), or public records sources. Additionally, each contractor has defined and documented procedures for claim form and payment creation, intake, and distribution (mail processing) to ensure accuracy within each matter. Because payments must be made to the eligible victim, the CFPB and its contractors take steps to ensure that information submitted by victims or obtained from other sources are verified for accuracy and completeness through validation. The victims may also have the opportunity to review and update their information.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that victims' PII may be inaccurate or incomplete.

Mitigation: The CFPB mitigates this risk by having contractors create standard processes for validating, scrubbing, and/or normalizing information received as part of a specific matter. In addition, contractors use internal systems and processes to identify information gaps and to complete missing data elements where possible and may, where necessary, rely on third party data providers. As part of these processes, the CFPB oversees all additions, deletions, and address changes to the information. In some cases, little to no victim's information is available, and the contractor is required to provide a method by which potential eligible victim can identify themselves and their claims for payment. In such cases, individuals providing their own

information are responsible for providing accurate information and the contractor and the CFPB are responsible for reviewing the claim's validity.

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 CFPB collects only the minimum amount of PII necessary for the management of civil penalty and redress funds, identification, and verification of harmed victims for payment, communication and help services for harmed victims, harmed victims claim processing, funds calculation, distribution, and tracking, and producing reports on fund administration. The information collected is retained according to the approved retention schedule.

The CFPB collects PII from harmed victims including basic information such as names and contact information for verification and payment of claims. The CFPB may also collect sensitive PII such as Social Security numbers and bank account information to locate and/or verify the identity of harmed victims for redress or compensation, to administer and track payments to harmed victims, and to meet reporting obligations. Some matters may require the collection of additional information such as benefits information in order to advise the harmed victim on how payouts may affect their need-based benefits.

The CFPB may also directly collect contact information of authorized third parties to facilitate communication or administration of payment on behalf of the harmed victim.

The CFPB may also collect PII about individuals with information, such as defendants and their employees, to a particular CFPB action. This is limited to basic contact 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 CFPB's Records and Information Management program collaborates with program managers to develop records retention schedules and submits them to the National Archives and Records Administration (NARA) for appraisal. NARA provides the authority to disposition when records retention schedules are approved.

The current NARA-approved records retention schedules for the Civil Penalty Fund and Redress Program are:

- Civil Penalties Program Working Files; DAA-0587-2014-0001-0001. **Disposition:** Maintain in office until no longer needed.
- Civil Penalties Closed Case Files; DAA-0587-2014-0001-0002. **Disposition:** Destroy 5 year(s) after penalty payment or OGC authorization.
- Civil Penalty Guidelines; DAA-0587-2014-0001-0003. **Disposition:** Destroy when no longer needed.
- Civil Penalty Fund Administrator; DAA-0587-2014-0001-0004. **Disposition:** Destroy/delete 3 years after cut-off.
- Financial Management Files; DAA-0587-2014-0001-0005. **Disposition:** Destroy/delete when no longer needed for reference, not to exceed discontinuance of program.

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

Privacy Risk: There is a risk that more information than necessary is collected from individuals.

Mitigation: This risk is mitigated by CFPB's general practice to always seeks the minimum amount of PII necessary to complete a task related to its mission. The PII collected for each matter is limited to only that which is necessary to complete tasks unique to that specific matter. For example, a matter where harmed victims are issued checks may only necessitate the collection of names and addresses of harmed victims; whereas a matter that involves payment through direct deposit, or in which CFPB has not been provided a list of harmed victims, a may require the collection of additional PII, such as a customer number or bank account number.

3. Uses of Information

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

When a person or company allegedly violates a federal consumer financial protection law, CFPB can bring an enforcement proceeding against them. If that person or company is found to have violated the law, it may have to pay a civil penalty, also known as a civil money penalty. When CFPB collects civil penalties, it deposits them in the Civil Penalty Fund. The CFPB

primarily uses the money in the Civil Penalty Fund to compensate victims harmed by activities for which civil penalties have been imposed. In cases where harmed victims cannot be located or such payments are otherwise not practicable, CFPB may use such funds for the purpose of consumer education and financial literacy programs. In order to compensate eligible victims, PII is collected to appropriately manage and administer CFPB's Civil Penalty and Bureau-administered Redress Program. The following tasks necessitate the collection of harmed victims PII:

- Fund management;
- Identification and verification of harmed victim for payment;
- Communication and help services for harmed victim and the public;
- Harmed victim claims processing;
- Funds calculation, distribution, and tracking; and
- Producing reports on the administration of funds.

Some matters may require individuals to verify their identity through a Social Security number or tax identification number or to provide additional sensitive information like marital status to ensure the CFPB meets any applicable tax-reporting obligations associated with the matter, or bank account information for victims to receive payments.

Additionally, some matters may also require collection of benefits and assistance information for CFPB and its contractors to determine whether a person may receive other government cash benefits after receiving civil penalty fund payments and also to inform harmed victims of how their eligibility for such need-based government benefits will be affected. The benefits information collected by CFPB contractors is limited to the minimum information needed as related to Civil Penalty Fund and redress payments. The information is only used for the purposes stated.

Finally, contact information of authorized third parties, such as a legal guardian or POA of the victim, is used to facilitate communication or administration of payment on behalf of the eligible victim. When a program-specific collection of data is proposed, the CFPB assesses the design and purpose of the program, including a collection of PII, through system design documentation reviews to verify that CFPB has an authorized purpose to collect and use the information.

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

Although it is not the practice of the Civil Penalty Fund and Redress Program to share information with other CFPB programs, there are instances where the program may need to conduct as-needed consultations with the CFPB Division of Enforcement. During such instances, information shared is limited to the minimum needed for the purpose of the consultation. The CFPB may use contractors and vendors to help support the collection, use, disclosure, or retention of information covered by this PIA.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risks: There is a risk that the information could be used for unauthorized purposes.

Mitigation: The CFPB mitigates this risk by implementing access controls within the system to ensure only authorized CFPB Staff[9] has access to the information. In addition, sensitive information is exclusively stored in systems (including contractor systems) with the requisite security authorization for holding this type of data. Where CFPB needs to share information with other individuals, this sharing occurs by directly connecting a CFPB or contractor system to those organizations' systems through secure methods or the transmission of information through secure channels. This sharing is consistent with routine uses identified within CFPB.025 - Civil Penalty Fund and Bureau-administered Redress Program Records SORN. When the CFPB uses contractors or vendors to assist with the program, those contractors or vendors are subject to similar administrative and technical controls as described below. Contractors may also be required to undergo training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations (FAR) and also go through an annual Authority to Use (ATU) process.

Privacy Risk: There is a risk that PII collected for the program will be shared with individuals that do not have a need to know and used in a manner that is inconsistent with the original purpose(s) for collection.

Mitigation: To mitigate this risk, the CFPB only shares information in accordance with laws, regulations, policies, and CFPB SORNs. 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 information maintained and review and acknowledge the Rules of Behavior for Privileged Users. The rules of behavior define the user's responsibilities, such as

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

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 when permitted by the CFPB's rules governing the Disclosure of Records and Information.[10] For example, confidential CFPB information may only be shared with CFPB employees, contractors, or consultants when such disclosure is relevant to the performance of their assigned duties.

Additionally, all CFPB Staff with access to CFPB systems under the Civil Penalty Fund and Bureau-administered Redress Program, 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 comply with privacy policy and complete privacy training when they initially onboard and on an annual basis thereafter. CFPB privacy training stresses the importance of appropriate and authorized use of personal information in government information systems.

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.

When PII is collected directly from harmed victims or third parties who represent the interest of eligible victims, notice is provided through a Privacy Act Statement at the point of collection. For example, some matters require a contractor to collect information directly from harmed victims to make payment using a form (either physical or an electronic web form). In these cases, notice is provided by a Privacy Act Statement on the form. Likewise, for matters where information is obtained directly from harmed victims through a consumer complaint filed with CFPB, notice is provided through a Privacy Act Statement via the CFPB online complaint form or telephone system. This Privacy Act Statement states CFPB's authority under which information is collected, purpose(s) for which the information is intended to be used, how the information may be disclosed,

[10] *See* 12 C.F.R. Part 1070.

applicable SORN, and the consequences for failing to provide information. Information obtained via consumer complaints is covered by the CFPB.005 – Consumer Response System SORN[11].

Individual notice is generally not provided for matters where the contractor receives information about harmed victims from a third-party data source not representing the victim or CFPB receives information directly from defendants. In such instances, the CFPB provides notice through the publication of this PIA and applicable SORN. If harmed victims become aware that their PII is being used, they may choose to opt out of this collection; however, that would make them ineligible for payment.

Additionally, for matters where a contractor uses an electronic web form on a website to collect PII from harmed victims, the CFPB requires that such websites include a privacy notice outlining how information collected by that website is stored, shared, and used. The CFPB also provides public notice about the program through this PIA and the SORN CFPB.025 – Civil Penalty Fund and Bureau-administered Redress Program Records.

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.

The CFPB collects PII about harmed victims through a variety of sources depending upon the nature of the matter. In general, when information is collected directly from harmed victims or authorized third parties acting on behalf of the victim (*e.g.,* POA), the CFPB provides notice that informs them that they may refuse to provide PII and the associated consequences. However, harmed victims whose PII is provided by a defendant directly to CFPB or provided by a third party not representing the victim, generally may not be aware of such collection and as such will not have an opportunity to consent. In some cases, harmed victims receive notice that a third-party contractor or vendor is verifying their claim (and any associated PII). In such cases, they may choose to opt out of this additional collection, but as a result, may not be eligible for payment. Harmed victims generally do not have the opportunity to consent to particular uses of their PII, regardless of how it is collected.

[11] *See* CFPB.005 Consumer Response System at https://www.consumerfinance.gov/privacy/system-records-notices/consumer-response-system/

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

Contractors provide harmed victims a method for direct contact in order to verify or correct collected information related to a specific matter.

Regardless of citizenship, individuals may request access, amendment, or correction to their records maintained by the program by contacting the CFPB's Freedom of Information Act (FOIA) Office[12] 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. The access, notification, and contesting procedures are also available through the SORN CFPB.025 – Civil Penalty Fund and Bureau-administered Redress Program Records. If you have any questions, please contact the CFPB FOIA Office via FOIA@CFPB.gov or at (855) 444-3642. Some source records, such as those related to a CFPB enforcement action, may not be subject to access or amendment.

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that harmed victims who have their information provided to CFPB or a contractor directly by a defendant may not have the same ability to opt out or decline to provide information as harmed victims whose information is collected directly.

Mitigation: The CFPB has mitigated this risk by requiring, for some matters, that contractors provide a method for harmed victims to contact a contractor directly to verify or correct information about them relative to a specific matter. This method, usually in the form of a direct mailing or a website, also contains additional information about the matter and harmed victims' rights concerning participating or not participating in the matter. In addition, the CFPB offers a means through the Privacy Act for individuals to access, amend, or correct their records maintained by the program. Information about access, notification, and contesting procedures for Privacy Act requests is available through the CFPB SORN, CFPB.025 – Civil Penalty Fund and Bureau-administered Redress Program Records. However, some source records, such as those related to a CFPB enforcement action, may not be subject to access or amendment.

[12] https://www.consumerfinance.gov/foia-requests/submit-request/

Privacy Risk: There is a risk that harmed victims do not have an opportunity to consent to particular uses of their PII.

Mitigation: This risk is however accepted under CFPB's mission and business practices, and if individuals become aware that their PII is being used, they may choose to opt out of this collection, thereby making them not eligible for payment. The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

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.

In instances as listed below where CFPB may have to share PII maintained within the program with third parties, that information is most often shared with consent from the harmed victim and via a secure channel. However, PII may also be shared when CFPB otherwise has the authority to do so, or pursuant to routine uses published in CFPB SORN, CFPB.025 – Civil Penalty Fund and Bureau-administered Redress Program Records. For example, as necessary, CFPB or a contractor managing a specific matter may share harmed victim information with:

- An entity or person that is the subject of a judicial or administrative action resulting in an order to pay civil penalties or redress to CFPB, and the attorney or non-attorney representative for that entity or person;
- The Treasury Department, Internal Revenue Service, or other governmental entities, including state and local taxing officials, to comply with tax-reporting obligations;
- A financial institution holding Civil Penalty Fund or redress monies on behalf of CFPB to issue payments to identified victims and for fraud protection. This information is sent via a secure channel by a vendor on behalf of the CFPB and is limited to names, amount paid, and check number;
- The CFPB's Office of Inspector General, the Government Accountability Office, or other governmental entities as necessary to comply with reporting obligations regarding the disbursement of Civil Penalty Fund or redress monies. Information is limited to audit records; and,
- The Federal Deposit Insurance Corporation (FDIC) to make claims under the FDIC's deposit insurance claims process, in the event that a financial institution holding Civil

Penalty Fund or redress monies on behalf of CFPB fails. The CFPB provides names of harmed victims who may need more protection to their accounts than is normally provided by FDIC.

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

Yes. The CFPB shares information as authorized in the published routine uses within the CFPB.025 - Civil Penalty Fund and Bureau-administered Redress Program Records SORN.

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

Privacy Risk: There is a risk that information may be shared in a manner that is inconsistent with the original collection.

Mitigation: The CFPB mitigates this risk by implementing administrative and technical access controls that help to ensure information maintained within the program is used according to the purposes identified in this PIA and other related notices. Only CFPB Staff has direct access to all the information collected and maintained. As information is shared with external parties when CFPB has the authority to do so, on a need-to-know basis, or pursuant to routine uses published in the CFPB.025 – Civil Penalty Fund and Bureau-administered Redress Program Records SORN, and the CFPB's regulations on Disclosure of Records and Information.

Privacy Risk: There is a risk of unauthorized access or use by individuals without a need-to-know.

Mitigation: The CFPB mitigates this risk by implementing security and privacy safeguards to protect CFPB systems and the information maintained within them. The CFPB uses the following technical and administrative controls to secure data and create accountability for CFPB's appropriate collection, use, disclosure, and retention of information:

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to the Civil Penalty Fund system and the data within.
- CFPB incident response procedures and privacy breach response procedures are in place to address the loss of control, compromise, or unauthorized disclosure of data residing in the Civil Penalty Fund system.

- Compliance with CFPB cybersecurity policies and procedures is documented within security and privacy implementation plans.
- Data quality and integrity checks are performed in accordance with CFPB's Data Access Policy for any systems using data within the program.
- Extract logging and reviews to ensure that data within the system is only accessed and used by authorized CFPB Staff.
- Personnel Security, including background checks, is completed for all CFPB Staff authorized to complete CFPB activities within the program.

The CFPB requires that all contractors supporting the Civil Penalty Fund and Bureau-administered Redress Program receive authorization from the CFPB cyber security team prior to rendering services under the program. Contractors may receive this authorization after CFPB review of the contractor's Third-Party Security Assessment – Statements on Standards for Attestation Engagements (SSAE), system security plans, evaluation of contractor responses to the Bureau-provided Self-Assessment security questionnaire, Plans of Action and Milestones (POAMs) provided by the contractor, and existing authorization letters from other agencies. Each contractor is evaluated separately through this process. Additionally, the CFPB has evaluated its own internal systems in an effort to ensure personal information is protected and determined that there is limited risk due to the technical and administrative controls implemented by CFPB.

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,[13] the Right to Financial Privacy Act,[14] and Section 208 of the E- Government Act of 2002. To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopts the Fair Information Practice Principles (FIPPs) as the framework for its privacy policy.[15] 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,

[13] 5 U.S.C. § 552a.

[14] 12 U.S.C. §§ 3401-3423.

[15] *See* CFPB Privacy Policy (Dec. 6, 2012), and subsequent updates.

regulations, and policy requirements.

The CFPB also adheres to the Office of Management and Budget privacy- related guidance[16] as a best practice; and applies the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)[17] for information technology systems, applications, solutions, and services. The CFPB identifies and applies NIST SP-800-53[18] 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.

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

The CFPB provides its Staff with appropriate privacy and security training to ensure information is used and secured appropriately and access controls are implemented by the system owner to ensure only those with authorized access can use the data. 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 general and role-based privacy training is required prior to granting access to the program's system. Role-based training includes data handling procedures, incident, and breach response procedures, and CFPB's authority to collect and use information in accordance with its regulations.

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

CFPB employs and uses role-based access controls to ensure CFPB Staff only have access to the system and/or information necessary and relevant to their assigned duties. Only CFPB Staff acting on behalf of CFPB have access to the systems under the program, which may include authorized staff from the contractor to provide technical support. No other systems or individuals

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

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

[18] *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.

have access to the data used by the program. The CFPB 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. Roles within the program's system include:

- Financial and Policy Analysts: Provides technical assistance and advisory services in accounting, budget analysis, financial management policies/issues, and compliance with applicable laws, regulations, and CFPB objectives. Permissions are based upon assigned business function and security configurations are based on their business and security needs within system.

- System Administrator role – A privileged role granted to authorized CFPB Staff, giving them full access to manage configuration settings within the system and manage user account privileges and permissions.

- Team Lead – Civil Penalty Fund – This is a general access role assigned to the team lead to manage the program.

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 in each contractor system 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, 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, CFPB Staff is assigned a unique user ID and password for access to systems. For contractors, information security policies exist for security administration, monitoring, and information security, and all contractor employees must complete mandatory security awareness training upon hire and annually thereafter. Access to any PII and other sensitive information is restricted and must be approved by the Program lead.

For PII that CFPB collects directly from a defendant, CFPB may need to transfer or share that PII directly with the contractor assigned to the specific matter to facilitate payment to harmed victims. This transfer occurs through secure channels that are assessed by CFPB cybersecurity and privacy risk management processes.

Document control

Approval

_____

Christopher Chilbert

Chief Information Officer

_____

Kathryn Fong

Chief Privacy Officer

_____

Rumana Ahmad

Team Lead - Governance, Compliance, and Civil Penalty

Original, signed document on file with the CFPB Privacy Office

Change Control

Version	Summary of material changes	Pages affected	Date of change
1.0	Original approval	All	August 2013
2.0	Discussion of the privacy risks and mitigations associated with the collection and use of PII, transferring into a new template, inclusion of NARA-approved record retention schedules, and general updates.	All	December 2023
3.0	Discussion of privacy risks associated with the collection of new PII, transfer into a newer template, and general updates.	All	November 2024