PRIVACY IMPACT ASSESSMENT— DECEMBER 2023

Civil Penalty Fund and Bureau-Administered Redress Program v.2

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Manage the distribution of Civil Penalty Fund and redress monies to consumers.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Generally applicable: Appropriate opportunities for notice, consent, access, and redress.

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). In executing its duties, CFPB collects information to successfully administer the Civil Penalty Fund and Redress Program (interchangeably referred to as "the Civil Penalty Fund and Redress Program" or "the program" hereafter).[1]

When a person or company 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 be required to pay a civil penalty, also known as a civil money penalty (CMP). CFPB collects and deposits the CMPs into its Civil Penalty Fund[2] and primarily uses these funds to financially compensate consumers harmed by illegal actions for which CMPs have been imposed. CFPB may also obtain other types of monetary relief, or redress, through judicial and administrative proceedings that CFPB uses to make payments to consumers harmed by a company or person's activities. This is called Bureau-administered Redress.

For all matters that result in redress or Civil Penalty Fund payments, CFPB is responsible for monitoring the distribution of funds held in the Civil Penalty Fund or in an account for Bureau-administered Redress to victims. CFPB's Chief Financial Officer is responsible for administering CFPB's Civil Penalty Fund and Bureau-administered Redress Program[3]. CFPB either directly manages the distribution of funds to 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:

- 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 generally the primary public contact for fund distribution activities. The contractor prepares public communications as described in the matter-

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 See 12 U.S.C. 5497(d).

3 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).

specific task order. The contractor's responsibilities include responding to public inquiries and addressing 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 victims have identified or verified themselves as a harmed consumer 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 victims as directed by 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 victim contact information.
- Reporting – For each assigned matter-specific task order, the contractor is required to provide 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.

Contractors may process and store, as necessary, information including personally identifiable information (PII) they receive either from CFPB, directly from victims, or from third parties. 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 in matter-specific systems such as:

- Database of potential and final funds recipients, their contact information, their potential and actual compensation amounts, successful and unsuccessful payment distributions, and any other relevant information for each matter;
- Potential recipients who inform the contractor, in writing, of their desire not to participate in the fund distribution;
- Potential recipients whose notification letters are undeliverable and potential recipients whose notification letters remain undeliverable even after attempts to obtain the corrected name and address information;

- Potential recipients who do not respond to the notification letter within the period specified for filing claims;
- Duplicate entries and claimants not eligible to receive a payment from a distribution;
- Potential recipients whose claim forms remain insufficient;
- All claims and supporting documentation submitted;
- Method and purpose of inquiries received from victims;
- Number of unique visits to the matter or claim website if one is developed; and
- Number and details of address changes submitted and updated.

Public Law 111-203, Title X, Sections 1017(d) (Civil Penalty Fund) and/or 1055(a) (Redress), codified at 12 USC §§ 5497(d), 5565(a), allow the information to be collected.

The CFPB is updating this privacy impact assessment (PIA) to discuss the privacy risks and mitigations associated with the collection and use of PII, to transfer into the new PIA template, to include the approved National Archives and Records Administration (NARA) record retention schedules, and to make several general updates as identified by CFPB's Privacy team and system owner. 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 civil penalty. Any PII or information collected to support those preceding activities are covered under separate PIAs. The CFPB's system of records notice (SORN), CFPB.025, Civil Penalty Fund and Bureau-Administered Redress Program Records gives notice of the information maintained and processed in the system. The information collected does not generally require approval under the Paperwork Reduction Act (PRA) as it does not meet the definition of a "collection of information" under 5 CFR 1320.3(c) requiring the Office of Management and Budget (OMB) clearance. However, in select claims cases where OMB approval is required, OMB Control Number 3170-0024 is used.

Privacy Risk Analysis

The primary privacy risks associated with this system are related to the following:

- **Limits on Uses and Sharing of Information**
- **Data Minimization**

- **Data Quality and Integrity**
- **Security**
- **Individual Participation.**

Limits on Uses and Sharing of Information

There are risks that the information could be used for unauthorized purposes. CFPB mitigates these risks by implementing access controls within the system to ensure only authorized staff 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, federal or state agencies, or private sector organizations, 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.

Data Minimization

There is a risk that more information than necessary is collected from individuals. 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 victims are issued checks may only necessitate the collection of names and addresses of victims; whereas a matter that involves payment through direct deposit, or in which CFPB has not been provided a list of victims, a may require the collection of additional PII, such as a customer number or bank account number. Additionally, 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 CFPB meets any applicable tax-reporting obligations associated with the matter.

Data Quality and Integrity

The CFPB collects PII of victims through a variety of methods. As a result, there is a risk that victims' PII may be inaccurate or incomplete. 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 relationships with third party data providers. 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. For example, prior to a contractor mailing a claim form, check, or educational material, victim 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. As part of these processes, CFPB oversees all additions, deletions, and address changes to the information. In some cases, little to no victim information is available, and the contractor is required to provide a method by which potential victims can identify themselves and their claims for payment. In such cases, individuals providing their own victim information are responsible for providing accurate information and the contractor and CFPB are responsible for reviewing the claim's validity.

In many instances, 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 other cases, contractors make claim forms available to previously unknown victims via a case-specific outreach effort, such as a dedicated website and web form. Again, victims provide information including their address, harm amount, and eligibility for payment. 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 victims to contact the contractor or CFPB to answer their questions or update their information. 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.

Security

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. The CFPB mitigates these risks in several ways. For example, 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, each employee 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 are required to complete mandatory security awareness training upon hire and annually thereafter. Access to any PII and other sensitive information is restricted and must be approved.

Individual Participation

There is a risk that 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 victims whose information is collected directly. The CFPB has partially mitigated this risk by requiring, for some matters, that contractors provide a method for 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 victims' rights concerning participating or not participating in the matter. In addition, CFPB offers a means through the Privacy Act for individuals to access, amend, or correct their records held in each system used for the program. Information about 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.

There is also a risk that victims do not have an opportunity to consent to particular uses of their PII. PII about victims is collected through a variety of sources depending upon the nature of the matter. In general, when information is collected directly from victims, CFPB provides notice that informs them that they may refuse to provide PII and the associated consequences. However, victims whose PII is provided by a defendant directly to CFPB or provided by a third party, generally may not be aware of such collection and as such will not have an opportunity to consent. However, this risk is 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.

Privacy Risk Management

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

The PII collected in the program comes directly from victims, defendants, or other third-party data sources.[4] 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). Victims can also provide information through a consumer complaint filed with CFPB. 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.

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

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

- Social Security number or tax identification number;

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

- 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, including employees, or other individuals associated with entities or defendants, may include:

- 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.

2. Describe CFPB's objective for the information.

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 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 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 victims PII:

- Fund management;
- Identification and verification of victims for payment;
- Communication and help services for victims and the public;
- Victim claims processing;

- Funds calculation, distribution, and tracking; and
- Producing reports on the administration of funds.

When a program-specific collection of data is proposed, CFPB assesses the design and purpose of the system, 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. Describe how CFPB shares any of the information with third parties with whom the CFPB shares the information for compatible purposes, e.g., federal or state agencies, the general public, etc.

In instances where CFPB may have to share PII maintained within the program with third parties, that information is most often shared with consent from the impacted individuals. However, PII may also be shared when CFPB otherwise has the authority to do so, or pursuant to routine uses published in our SORNs. As necessary, CFPB or a contractor managing a specific matter may share 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;
- The United States Postal Service (USPS) or other public directories to validate victim contact information or to comply with tax-reporting obligations as applicable;
- 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; 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 shares information as authorized in the published routine uses within the CFPB.025 - Civil Penalty Fund and Bureau-administered Redress Program Records SORN available at https://www.consumerfinance.gov/privacy/system-records-notices/civil-penalty-fund-and-bureau-administered-redress-program-records/.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c) access the information that pertains to them; or (d) obtain redress.

When PII is collected directly from 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 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 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.

For matters where the contractor receives information about victims from a third-party data source or CFPB receives information directly from defendants, notice is generally not directly provided. Notice is however provided through the publication of this PIA and applicable SORN. If victims become aware that their PII is being used, they may choose to opt out of this collection, thereby making them not eligible for payment.

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

In some cases, victims receive notice that a third party 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. Victims generally do not have the opportunity to consent to particular uses of their PII, regardless of how it is collected.

The CFPB offers a means through the Privacy Act for individuals to access, amend, or correct their records held in each system used for the program. Information about Privacy Act requests is available through the CFPB SORN, CFPB.025 – Civil Penalty Fund and Bureau-administered Redress Program Records. Contractors also provide victims a method for direct contact in order to verify or correct collected information related to a specific matter. Some source records, such as those related to a CFPB enforcement action, may not be subject to access or amendment.

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

The CFPB complies with the Privacy Act of 1974, the Right to Financial Privacy Act, and the E-Government Act of 2002; it voluntarily adopts Office of Management and Budget privacy-related guidance as a best practice; and applies the National Institute of Standards and Technology risk management processes for privacy.

The CFPB may collect PII about victims through a variety of methods. 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 victims. This transfer occurs through secure channels that are assessed by CFPB cybersecurity privacy risk management processes. 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, 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.

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 general and role-based privacy training is required prior to granting access to the ServiceNow platform and any applications within the platform. 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.
- 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 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.
- Role-based Access Controls: 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 Civil Penalty Fund 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.
- Records Schedule Approved by NARA:
    - Civil Penalties Program Working Files; DAA-0587-2014-0001-0001.

- Civil Penalties Closed Case Files; DAA-0587-2014-0001-0002.
- Civil Penalty Guidelines; DAA-0587-2014-0001-0003.
- Civil Penalty Fund Administrator; DAA-0587-2014-0001-0004.
- Financial Management Files; DAA-0587-2014-0001-0005.

- Personnel Security, including background checks, is completed for all employees, contractors, or individuals authorized to complete CFPB activities within the program.

The CFPB may use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA. Those contractors are subject to similar administrative and technical controls as described above. For example, contractors with access to direct identifying PII must report suspected or confirmed privacy incidents to CFPB no later than one hour after discovery. Contractors may also be required to undergo training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations (FAR).

The CFPB has updated this PIA as a result of its privacy continuous monitoring (PCM) processes. Various minor changes have been completed and the PIA has been redrafted using CFPB's new PIA template.

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf of the CFPB, e.g., government contractors discussed in Question 5.)

Only CFPB employees and contractors acting on behalf of CFPB have access to the system, which may include authorized staff from the vendor to provide technical support. No other systems or individuals have access to the data in the system.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2023.12.15 17:04:36 -05'00'

Christopher Chilbert

Chief Information Officer

Date

KATHRYN FONG

Digitally signed by KATHRYN FONG
Date: 2023.12.15 17:22:59 -05'00'

Kathryn Fong

Chief Privacy Officer

Date

RUMANA AHMAD

Digitally signed by RUMANA AHMAD
Date: 2023.12.14 14:33:27 -05'00'

Rumana Ahmed

Team Lead - Governance, Compliance, and Civil Penalty

Date

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 new PIA template, inclusion of NARA-approved record retention schedules, and general updates.	All	December 2023