AUGUST 16, 2013

Privacy Impact Assessment

CIVIL PENALTY FUND AND BUREAU-ADMINISTERED REDRESS PROGRAM

Contact Point:
Claire Stapleton
Chief Privacy Officer
1700 G Street, NW
Washington, DC 20552
202-435-7220
claire.stapleton@cfpb.gov

Consumer Financial Protection Bureau

DOCUMENT PURPOSE

The Privacy Impact Assessment or "PIA" provides the public with information about the Consumer Financial Protection Bureau's ("CFPB" or "Bureau") collection and use of personally identifiable information ("PII"). PII is any information "that can be used to distinguish or trace an individual's identity"[1] like a name, address, Social Security number, or place and date of birth. The CFPB uses PIAs to document how the PII it collects is used, secured, and destroyed in a way that protects each individual's privacy. Each PIA is broken out into sections that reflect the CFPB's Privacy Principles. The CFPB's Privacy Principles are a set of nine rules the CFPB follows when it collects or uses PII.

OVERVIEW

PROJECT / SYSTEM NAME: Civil Penalty Fund and Bureau-Administered Redress Program

PROJECT/SYSTEM INCLUDES INFORMATION ABOUT:

- ☒ Federal Employees
- ☒ Contractors
- ☐ Consultants
- ☒ The Public

PROJECT/SYSTEM INCLUDES:

- ☒ Name and other biographic information (e.g. date of birth)
- ☒ Contact Information (address, zip code, telephone number, email address)
- ☒ Social Security number ("SSN") or other identifier
- ☒ Financial Information
- ☐ User and Online Information
- ☒ Third party Information
- ☐ Other Information (including biometric information and health or medical information)

Civil Penalty Fund and Bureau-Administered Redress

When the CFPB takes an enforcement action against a person or a company for violating a federal consumer financial protection law, the person or company may have to pay a civil money penalty ("CMP"). The Bureau puts CMPs into its "Civil Penalty Fund,"[2] and primarily uses them to make payments to consumers harmed by illegal actions for which CMPs have been imposed. The Bureau may also obtain various types of other monetary relief, called "redress," through judicial and administrative proceedings. Redress money that has been paid to the Bureau is used to make payments to consumers harmed by a company or person's activities. This is called "Bureau-Administered Redress." You can read more about the Civil Penalty Fund at http://www.consumerfinance.gov/budget/civil-penalty-fund/ and about

---

[1] Office of Management and Budget ("OMB") Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, (OMB M-07-16) defines PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

[2] *See* 12 U.S.C. 5497(d).

Bureau-Administered Redress at
http://files.consumerfinance.gov/f/201307_cfpb_faqs_cpf.pdf.

Defined Terms

This document uses several common terms, defined below, in relation to the process of collecting, managing, and disbursing money through the Civil Penalty Fund and Bureau-Administered Redress Program.

- **Civil Penalty Fund and Bureau-Administered Redress Program** *or* "**the program**" – Any of the Bureau's Civil Penalty Fund or Bureau-Administered Redress activities, and all associated procedures, technologies, and contract support.
- **Claim –** The process of victims identifying or verifying themselves as a harmed consumer, and requesting payment from the Bureau's Civil Penalty Fund and Bureau-Administered Redress Program.
- **Contractor(s)** – Any third-party vendor, contracted by the Bureau to provide services (and perform tasks) related to the management of funds and distribution of funds to victims. In some cases, Contractors work with sub-contractors, partner vendors, and other third parties to facilitate the completion of the tasks outlined in this PIA. For the purposes of this assessment, such third parties are considered part of the "Contractors" referenced in this document.
- **Defendant(s) –** Any company or person ordered to pay a civil money penalty or redress) to the Bureau.
- **Funds –** Any monies that the Bureau holds in the Civil Penalty Fund or in an account for Bureau-Administered Redress.
- **Matter(s) –** Any case that results in redress or Civil Penalty Fund payments being made by the Bureau.
- **Task Order –** Any order from the CFPB to a Contractor for the performance of tasks, specific to a matter, related to the management of funds and distribution of funds to victims.
- **Victim(s) –** An individual who is the recipient or proposed recipient of payments through the Bureau's Civil Penalty Fund and Bureau-Administered Redress Program.

Program Management

For all matters, the Bureau is responsible for monitoring the distribution of funds to victims. The Bureau's Chief Financial Officer is responsible for administering the Bureau's Civil Penalty Fund and Bureau-Administered Redress Program.[3] In some cases, the Bureau will manage the distribution of funds to victims. In other cases, the Bureau issues task orders, specific to a matter, for a Contractor to provide some (or all) of the following services:

- **Funds management –**Contractors must manage specified funds related to a particular matter, which includes establishment of an account (to hold the funds) and reporting.
- **Communication and help services for consumers and the public –** For each assigned matter, the Contractor will generally be the main public point-of-contact as related to fund distribution activities. The Contractor will prepare public communications as described in

[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).

the matter-specific task order. The Contractor's responsibilities will include responding to general 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.
- **Funds distribution –** The assigned Contractor will distribute funds from the established account to victims as directed by the Bureau through the specific task order. Each matter will require the maintenance of a specific system(s) tracking contact information and payment information. Additionally, in some instances, the Contractor will be required to locate victim contact information, in a timely and cost-effective manner.
- **Reporting –** For each assigned matter-specific task order, the Contractor will be required to provide the Bureau with monthly and ad hoc reports on activities, including funds distribution, tracking and public communication. Additionally, the Contractor may be required to provide tracking and 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 Bureau has Contractors provide these services on a task order basis. Each Contractor processes (and stores as necessary) information that it receives from the Bureau, directly from victims, or from third parties in matter-specific databases (called "systems") in secure on-site and off-site locations. The systems created and/or used by Contractors will vary based on the nature of the matter, but in general, Contractors will 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 corrected name and address information;
- Potential recipients who do not respond to the notification letter within the time 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.

The Bureau is conducting this PIA to evaluate the collective impact these systems and related procedures involved in the overall Bureau Civil Penalty Fund and Bureau-Administered Redress Program have on personal privacy. Additionally, the Bureau has a process in place by which members of its Privacy and Cyber-Security teams review each task order issued by the Bureau to Contractors relative to the program for consistency with the statements made in this document.

SECTION 1.0 PURPOSE OF COLLECTION

The CFPB will state the purpose and legal authority for collecting PII.

1.1 Why is the information being collected?

The Bureau and Contractors collect PII to appropriately manage the Bureau's Civil Penalty and Bureau-Administered Redress Program, including:

- Fund management
- Communication and help services for victims and the public
- Victim claims processing
- Funds distribution
- Reporting

More information about each of these components is available in the introductory section of this document.

1.2 What legal authority and/or agreements allow the information to be collected?

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

1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

Yes. Systems used for the program are covered by the CFPB's System of Records Notice, CFPB.025 – Civil Penalty Fund and Bureau-Administered Redress Program Records.

1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration (NARA) for the information system(s)? Explain how long and for what reason the information is retained.

The CFPB will manage all computer and paper files in the program as permanent records until the disposition schedule for these records is approved by the National Archives and Records Administration, at which time, the CFPB will dispose of such files in accordance with the schedule.

1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act (PRA)?

As of publication of this document, there are no forms or surveys associated with the program that would be covered by the PRA. If such forms are created or necessary for the program in the future, the CFPB will modify this PIA to reflect them.

1.6 Are there any privacy risks for this system that relate to

the purpose of the collection? If so, how will the CFPB mitigate these risks?

No.

SECTION 2.0 OPENNESS AND TRANSPARENCY

The CFPB will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.

2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.

When the Bureau or a Contractor collects PII for the program, they do so through a variety of methods. In general, 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 in order 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 the Bureau, notice is provided through a Privacy Act Statement via the CFPB online complaint form or telephone system.

For matters where the Contractor receives information from a third-party data source or the Bureau receives information directly from defendants, notice is generally not provided. For example, for matters where the Contractor uses a third-party data source, including public-record sources, such as the United States Postal Service's ("USPS") National Change of Address Database ("NCOA") or LexisNexis (for address corrections, etc.), notice is not provided at the time of collection.

Additionally, for matters where a Contractor uses an electronic web form on a website to collect PII from victims, the Bureau requires that such websites include a privacy policy outlining how information collected by that website is stored, shared, and used.

The Bureau also provides constructive notice about the program through this PIA and through the CFPB SORN, CFPB.025 – Civil Penalty Fund and Bureau-Administered Redress Program Records.

2.2 Will individuals be given notice prior to their information being shared? If not, please explain.

As discussed in Section 2.1, for matters where the Bureau or Contractors collect information directly from victims, notice is generally provided through a Privacy Act Statement, and, as necessary, a privacy policy when victims provide information through a Contractor-operated website. In cases where information about victims is collected by the Bureau from the defendant or by a Contractor from a third-party data source, no direct notice is provided.

The Bureau also provides constructive notice through this PIA and through the CFPB SORN, CFPB.025 – Civil Penalty Fund and Bureau-Administered Redress Program Records.

Section 4.2 discusses the limited ways in which the CFPB will share PII from the program.

2.3 Are there any privacy risks for this system that relate to openness and transparency? If so, how will the CFPB mitigate these risks?

There is a risk that victims do not receive direct notice of the collection or use of their PII when that information is provided directly by the defendant to the CFPB or by a third party to a Contractor managing a specific matter. The CFPB has partially mitigated this risk by:

- Providing notice through this PIA;
- Providing information about the Civil Penalty Fund and Bureau-Administered Redress Program on its website, www.consumerfinance.gov;
- Providing victim educational materials (distributed by Contractors managing specific matters); or
- Developing matter-specific websites which contain more information on a specific matter or provide a method for contacting a Contractor directly to verify or correct information about them (relative to a specific matter).

SECTION 3.0 DATA MINIMIZATION

The CFPB will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. The CFPB should keep PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system?

The types of individuals whose PII is collected, used, disseminated, or maintained either by the Bureau or within the Contractors' systems vary depending upon the matter, but in general include:

- Victims or possible victims who may receive payments from the Civil Penalty Fund or through Bureau-Administered Redress; and
- CFPB employees and others, including employees of and other individuals associated with defendants with information relevant to, or otherwise associated with, a Bureau action that has resulted in an order to pay CMPs or redress to the Bureau.

3.2 What PII will the system include?

PII about victims collected, used, disseminated, or maintained either by the Bureau or within the Contractors' systems varies depending upon the matter, but in general, includes:

- First, middle, and last name
- Address and contact information including:
- Street address
- City, state, ZIP code, country
- Home and work phone number
- Email addresses
- Transaction or claim information including:
    - Transaction dates
    - Company selling product and product type
    - Customer number or account number
    - Harm amount
- Internal identification number assigned to identified victims

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

- SSNs or tax identification numbers
- Date of birth ("DOB")
- Marital status
- Credit card numbers and card issuer names
- Bank account numbers and bank names

PII about other individuals with information relevant to a Bureau action that has resulted in an order to pay CMPs or redress to the Bureau, including employees or others associated with defendants, may include:

- First and last name
- Position or title
- Work address and contact information including:
- Street address
- City, state, ZIP code, country
- Home and work phone number
- Email addresses

3.3 Why is the collection and use of the PII necessary to the project or system?

As discussed in Section 1.1, the collection and use of PII is necessary to manage the Bureau's Civil Penalty Fund and Bureau-Administered Redress Program, including:

- Fund management
- Communication and help services for victims and the public
- Victim claims processing
- Funds distribution
- Reporting

This includes identifying and verifying victims for payment; calculating, distributing, and tracking those payments; and providing reports about administration of the funds. Depending on the nature of the specific matter, this effort may include a combination of:

- Printing and mailing claim forms or creating an electronic web form on a website
- Processing claims and corrections submitted by victims
- Issuing checks and other forms of payment
- Providing consumer education and notification
- Producing reports on disbursement of funds or reports to meet tax-reporting obligations

3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?

No.

3.5 What controls exist to protect the consolidated data and prevent unauthorized access?

Systems used to support the program do not consolidate or create new data. Section 6.0 of this PIA discusses controls generally applied across all systems supporting the program.

3.6 Will the system monitor the public?

No.

3.7 Will the system monitor employees or contractors?

Bureau and Contractor employees are subject to monitoring in regards to their access to or use of systems used in managing the program. In general, such monitoring is limited to each employee's appropriate use of a system and any information contained within or used by that system.

3.8 What kinds of reports can be produced on individuals? Will the data included in the reports produced be made anonymous?

Each system can produce reports to support the various purposes of the program. Reports vary depending on the nature of a specific matter and the system used to support that matter. In general, there are two broad categories of reports generated on a regular basis to support the program:

- **Performance Reports –** Contractors provide reports about their level of performance in regards to specific matters. For example, Contractors produce monthly status reports on all on-going work pertaining to specific matters. These reports may include limited PII about Contractor employees assigned to a specific matter, but are not specifically about individual employees. Rather, such reports are about the Contractor's completion of specific tasks related to the matter, such as identifying victims or disbursing funds.
- **Matter-specific Reports –** Systems supporting the program may generate a variety of reports related to a specific matter. These reports may include PII about victims involved in a specific matter, such as victims who receive or decline payment as part of a specific matter, or victims who cannot be located, or reports generated to help the Bureau meet tax-reporting obligations. The introductory section of this PIA provides a generalized list of the types of systems created and maintained in support of the program.

The CFPB may also request, as necessary, a complete and secure download file of matter-specific information, which includes PII about specific victims receiving payment.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will the CFPB mitigate these risks?

No.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

The CFPB will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the

collection?

As discussed in Sections 1.1 and 3.3, all PII collected or used is necessary and relevant to managing the program, including the completion of tasks related to a specific matter. 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 the defendant has not provided a list of victims and such victims must self-identify through claims process, 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 SSN or tax identification number, or to provide additional sensitive information like marital status to ensure the Bureau meets any applicable tax-reporting obligations associated with the matter.

4.2 Will the CFPB share any of the information with other individuals, federal and/or state agencies, or private sector organizations? If so, how will the CFPB share the information?

As necessary, the CFPB or a Contractor managing a specific matter may share information with other individuals, federal or state agencies (including taxing agencies), or private sector organizations, like the USPS or LexisNexis to validate victim PII contact information or to comply with tax-reporting obligations as applicable. This sharing will occur by directly connecting a CFPB or Contractor system to those organizations' systems through secure methods, or through transmission of information through secure channels, such as File Transfer Protocol ("FTP").

4.3 Is the information collected directly from the individual or is it taken from another source?

As discussed in Section 2.1, in some cases, Contractors or the Bureau may collect PII directly from victims. In other cases, the Bureau collects PII about victims directly from the defendant. Sometimes a Contractor may need to collect additional PII about victims from third-party data sources. This is generally limited to address and other contact information corrections to facilitate identification or verification of, and payment to, victims.

The Bureau or a Contractor collects PII by a variety of methods, depending on the nature of the specific matter, including complaint forms, correspondence, telephone calls, fax submissions, web forms, and other web-based information collection.

4.4 Will the project interact with other systems, whether within the CFPB or outside of the CFPB? If so, how?

As discussed in Section 2.1, Contractors or the Bureau may collect PII about victims through a variety of methods. For PII that the Bureau collects directly from a defendant, the Bureau 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 from the Bureau's systems to the Contractor's systems through secure channels. Sometimes a Contractor may need to collect additional PII about victims from third-party data sources such as USPS or LexisNexis to facilitate correction or validation of victim information. In doing so, the Contractor may make secure connections between these systems and their systems to send relevant data elements to match records for verification purposes. In other matters, the Bureau or a Contractor may

need to provide PII to other governmental entities, including taxing officials, to comply with tax-reporting obligations. Such sharing will occur through secure methods.

4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will the CFPB mitigate these risks?

No.

SECTION 5.0 DATA QUALITY AND INTEGRITY

The CFPB will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

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 education material, victim addresses are standardized and validated against known data sources, such as the USPS NCOA, or public records sources such as LexisNexis. The CFPB approves all additions, deletions, and address changes to the information and reconcile the revised information against the original source information. In cases where the Contractor must coordinate the identification of victims, the CFPB will validate all claims (and related information) prior to payment being distributed.

In many instances, the Bureau 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, under penalty of perjury, information including their address, harm amount (amount lost as a result of a defendant's violation of 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 under penalty of perjury.

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 the CFPB to have their questions answered or to 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.

5.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will the CFPB mitigate these risks?

There is a risk that victims' PII may be inaccurate or incomplete. The Bureau has mitigated this risk by having Contractors create standard processes for validating, scrubbing, and/or normalizing information received as part of a specific matter. 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, such as the USPS or LexisNexis to ensure victims' information is accurate and complete. As part of these processes, the CFPB approves all additions, deletions, and address changes to the information and reconciles the updates against the original source 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.

SECTION 6.0 SECURITY

The CFPB must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who will have access to the data in the project? What is the authorization process for access to the project?

The CFPB and each Contractor managing systems used by the program have implemented robust security controls, both physical and technical, for the environment housing each system.

Physical Controls to Limit Access

Only authorized individuals are permitted to enter CFPB or Contractor facilities, which are guarded and monitored for unauthorized physical access. CFPB and Contractor employees are subject to background checks upon hire and are issued physical access badges for entry into relevant facilities.

Additionally, certain portions of Contractor facilities are subject to additional restrictions for access. For instance, access to check-printing rooms (where victims' checks are printed for distribution), or the mail processing area, is limited to a subset of authorized Contractor personnel who have a need to access those spaces, which have their access controlled by electronic security systems. Visitors to each Contractor facility are only permitted access when escorted, after having been approved by management and issued visitor access badges.

Technical and Administrative Controls to Limit Access

The CFPB and each Contractor have implemented technical controls to assure that access to systems, computer programs and information prevent or detect unauthorized access or changes to those systems, programs, or information.

The CFPB and each Contractor limit access to information in the project 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.

6.2 Has the CFPB completed a system security plan for the information system(s) supporting the project?

The CFPB is doing a Third Party Security Assessment – Statements on Standards for Attestation Engagements ("SSAE") 16 Review. This review includes evaluating each Contractor's response to the Bureau-provided Self-Assessment security questionnaire, Contractor-provided Plans of Action and Milestones ("POAMs"), and existing Authority to Operate ("ATO") letters from other agencies. Each Contractor providing support is evaluated separately through this process. Additionally, the Bureau has evaluated its own internal systems.

6.3 How will the system be secured?

Information in each Contractor system is protected through robust security controls 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). Required security for each component is derived from the sensitivity of the information within that component.

Additionally each Contractor is responsible for implementing policies and procedures that ensure the security of its systems and any information housed within each of those systems.

The Bureau and Contractors periodically review their systems and processes, and each may be subject to additional assessment under each task order issued. Section 6.1 further discusses access and related security controls for the program.

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

In general, the CFPB follows the Treasury Department's directives related to security and privacy incidents. The CFPB has developed supplemental interim incident-reporting materials, and, upon moving onto its own network infrastructure, will issue new directives related to security and privacy incidents.

Additionally, each Contractor is required to have developed and implemented policies and procedures for detecting and reporting security incidents and other anomalies. This includes sending the CFPB monthly vulnerability scan results, any "applicable" incident reports as needed, and the results of annual incident response tests. The CFPB works closely with each Contractor to develop a plan by which the Bureau is notified (in a timely matter) of potential incidents which may warrant further reporting or escalation.

6.5 Are there any privacy risks for this system that relate to security? If so, how will the CFPB mitigate these risks?

No.

SECTION 7.0 INDIVIDUAL PARTICIPATION

The CFPB will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

As discussed in Sections 2.1 and 4.3, PII about victims is collected through a variety of methods, depending upon the nature of the matter. In general, victims who receive a Privacy Act Notice when their PII is collected are informed that they may refuse to provide PII, and the associated consequences, whereas victims who have their PII provided by the defendant directly to the Bureau, or have it provided by a third party to a Contractor, generally do not have such an opportunity. 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.

In general, victims do not have the opportunity to consent to particular uses of their PII, regardless of how it is collected.

7.2 What procedures will allow individuals to access their information?

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. Additionally, as discussed in Section 5.1, Contractors provide victims a method for contacting them directly to verify or correct information about them relative to a specific matter. Some source records, such as those related to a CFPB enforcement action, may not be subject to access or amendment.

7.3 Can individuals amend information about themselves in the system? If so, how?

Sections 7.2 and 5.1 address how individuals may access and amend their records in the system.

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will the CFPB mitigate these risks?

There is a risk that victims who have their information provided to the Bureau or a Contractor directly by a defendant may not have the same ability to opt-out or decline to provide information as victims who have their information collected directly from them. 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. Additionally, this method, which is 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 as outlined in Sections 7.1 and 7.2.

There is also a risk that victims do not have an opportunity to consent to particular uses of their PII. In general, individuals consent to their information being provided for all uses described in the applicable privacy policies provided at either the time of collection of the information, or as outlined in the SORN, CFPB.025 – Civil Penalty Fund and Bureau-Administered Redress Program Records. The Bureau has accepted this risk in order to facilitate operations and because the impact to personal privacy is minimal.

SECTION 8.0 AWARENESS AND TRAINING

The CFPB will train all personnel about the proper treatment of PII.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

The CFPB offers general privacy and security training to all employees of the CFPB, including Contractors who handle PII on behalf of the Bureau.

Additionally, each Contractor, as part of a rigorous set of security controls, requires its employees to complete annual security awareness training and abide by the Contractor's security policies and protocols. Furthermore, Contractor employees may receive additional training relevant to their particular duties, as they relate to security and privacy. For instance, contact call center employees (who answer questions about claims or take information for claims from victims) receive specialized training on how to intake information from and deliver accurate information to callers.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will the CFPB mitigate these risks?

No.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

The CFPB is accountable for complying with these principles. We will regularly check that we are meeting the requirements and take appropriate action if we are not doing so.

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

The CFPB, and Contractors managing matters on its behalf, has implemented controls as outlined in this PIA to ensure the confidentiality, accuracy, and integrity of information in each system and throughout the program at large. Additionally, the CFPB has integrated a process by which certain task orders issued to Contractors are reviewed by members of the Bureau's Privacy and Cyber-Security teams to ensure concurrence with the statements made in this document and to address any new or additional risks posed by each task order.

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will the CFPB mitigate these risks?

No.