PIA Title v.#

Does the CFPB use the information to benefit or make a determination about an individual?	Yes/No
What is the purpose?	Illustrative: Resolve complaints regarding financial products.
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,

KEY FOR USING THIS TEMPLATE

All template text is header format. All other text is guidance designed to help the System Owner or Program Manager to complete the PIA template. Special guidance for specific types of activities is provided in color-coded sections.

Normal: General guidance

Bold: Always required

> Third-party websites or applications

> Information disclosures

> Agile development, system change requests (CR), security assessment and authorization (SA&A) packages

~~Strikethrough~~: Considered, no additional detail required; or Not Applicable

For the purposes of this PIA template, there are four categories of third parties: 1) Contractor(s) acting on behalf of the CFPB; 2) Collaborator(s) or partner(s) with whom the CFPB must work with in order to collect, use, disclose, retain, or dispose of the information; 3) Third party (ies) with whom the CFPB shares the information for compatible purposes, e.g. federal agencies through Routine Uses of the applicable SORN; and 4) Third party (ies) that host websites or applications.

Overview

In plain language, describe the **legal authority and/or agreements applicable** to the Initiative; the lifecycle of the information; program management of the Initiative; or the concept of operations for any technology enabling the Initiative. Define the scope of the PIA, identifying any limitations or overlaps with other PIAs. **Explain why the information is being**

collected and how it will be used. Explain whether a System of Records Notice (SORN) is required; if so, cite; if not, explain. Explain whether a PRA approval is required; if so, cite; if not, explain.

The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the Initiative.

> As appropriate, affirm in the PIA that for agile development, system change requests (CR), and security assessment and authorization (SA&A) documentation addresses privacy relative to systems development, including, as warranted and appropriate: statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment.

> For disclosures of information, explain the role of disclosure relative to the rest of the information lifecycle. Explain whether the disclosure is a single information disclosure or a series of disclosures with substantially the same content.

Privacy Risk Analysis

This discussion is intended to summarize any key privacy risks raised by the questions below, and the Bureau's mitigation efforts with respect to those risks. Discuss key privacy risks related to this Initiative. Where applicable, consider the privacy risks related to:

- **Purpose of Collection**
- **Openness and Transparency**
- **Data Minimization**
- **Limits on Uses and Sharing of Information**
- **Data Quality and Integrity**
- **Security**
- **Individual Participation**
- **Awareness and Training**
- **Accountability and Auditing**

Identify any potential privacy-related harm, e.g. identity theft, embarrassment, loss of reputation, loss of benefit, etc. that an individual may experience as a result of the collection, use, or sharing of information. Discuss any measures taken to ensure sufficient data quality and

integrity of information necessary to achieve the purpose of collection; in particular, explain any measures taken to improve data quality and integrity that reduce the risk that an individual may be negatively impacted. Where applicable, address the alternatives to collection and handling of personal information as designed, the appropriate measures to mitigate risks identified for each alternative, and the rationale for the final design choice or business process. While privacy impact in all stages of the information lifecycle (i.e. collection, use, retention, processing, disclosure and destruction) should be considered, the discussion here should only address those stages that present privacy risk. Address only relevant stages of the information lifecycle or concept of operations. Consider whether the use of the information creates previously unknown information about an individual or generates profiles about individuals' behaviors or social relationships (e.g., data mining). Explain whether the project involves the CFPB's first use of a given technology.

If accurate, end this section with the following statement: "The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate."

> For Agile development, system CRs, and SA&A packages, address the impact the system/technology will have on an individual's privacy, to the extent these elements are known at the stages of development.

> For disclosures of information, discuss the probability of re-identification by looking at risks internal to the dataset such as links between participants where the characteristics of one individual may facilitate the identification or association of characteristics to another individual in the dataset. Also consider risks external to the dataset, such as matching with commercially or publicly available datasets. Publicly available datasets may include, but are not limited to: vehicle registration lists; voter registration lists; federal, state, or local tax records; criminal justice system records; state hunting and fishing license registers; membership rosters of associations; and survey data that share the same samples.
>
> Where relevant, consider: 1) the number of variables available for matching purposes, 2) the resources needed to perform the match, 3) the age of the data, 4) the accessibility, reliability, and completeness of the external file, and 5) the sensitivity or uniqueness of the data.

> Where relevant, evaluate data for risks of re-identification of individuals. Cite and discuss any relevant standards or policies that apply to the disclosure of information. Disclosure criteria for micro data may vary by dataset. Where relevant, evaluate data for risks of re-identification of individuals based on geographic indicators (e.g., zip code); unique personal characteristics (e.g., high income, old age, language spoken, racial identification, value of property, rent or mortgage); contextual or ecologic variables (e.g., census tract or block group, rate of employment); or receipt of public assistance.

Privacy Risk Management

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

Describe what information CFPB collected and from where. Consider information collected directly from the individual by phone, mail, online, or in person. Consider information received from government sources such as federal and state financial regulators. Consider non-government sources such as members of the public, media/internet, private sector, and commercial data brokers.

> For third party websites or applications, describe the selection criteria for that third party website or application, and any PII that is likely to become available to the agency through public use of the third-party website or application.

> For disclosures, explain whether CFPB collects the information directly from an individual or receives it from a third party. Discuss whether disclosure is a secondary purpose or use of the information, and if so, identify the primary purpose of the collection of information.

Where applicable, identify any forms or surveys used in the collection.

Address the consequences of collection and flow of information. Explain how the collection of information is minimized to what is necessary for the purpose of the collection.

2. Describe CFPB's objective for the information.

Describe CFPB's primary uses of the information. Also describe relevant uses of the information by any third-party partners or collaborators, not acting directly on behalf of CFPB, but whose participation is necessary for CFPB's use of the information. An example of a third-party partner or collaborator is: after an open selection process, the CFPB partners with a financial service provider to test whether certain interventions improve savings outcomes. Explain how the uses and disclosures are limited to authorized uses and compatible purposes. Discuss how the use of each data element or category of data elements is both relevant and necessary to the purpose for which it is collected. For example, Social Security Numbers (SSNs) should only be collected when explicit authority to collect and use it exists and not because the SSN is a convenient way to uniquely identify individuals.

> If the CFPB is using a website or application hosted on a third-party site using web measurement and customization technologies to which Federal privacy and data safeguarding standards do not apply, explain why the decision was made to use a third party site using web measurement and customization technologies; and how the CFPB provides the public with alternatives for acquiring comparable information and services.

> Describe the purpose for disclosing the information, i.e. the utility of the information by users external to CFPB, and any restrictions on the use of information by users external to CFPB.

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.

If applicable, how does the CFPB intend to share the information with third parties? Describe how the information is disclosed, and any limitations related to

disclosure. For example, discuss any applicable licensing agreement; terms of use; non-disclosure agreements, confidentiality statements, application programming interface, remote data center, data query model, etc. **If governed by a System of Records Notice, discuss the relevant Routine Uses. Discuss any interaction with other systems or programs, whether within the CFPB or outside of the CFPB.** This discussion generally would not include sharing with contractors acting on the CFPB's behalf.

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.

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. Consider opportunities and limitations provided through the SORN, Privacy Act Statements or Privacy Notices, or applicable Privacy Policies. When any of the opportunities (a)-(d) are not provided, discuss mitigation of any applicable privacy risks. When a SORN is applicable, typically include: "The CFPB gives individuals the ability to request access and amendment to their personal information in accordance with the Privacy Act and the CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq."

> If accurate, explain how appropriate Privacy Notice was given on the third party website or application; and affirm that the use of the third party website or application is addressed in the CFPB's Privacy Policy in accordance with OMB Memorandum 10-23, "Guidance for Agency Use of Third-Party Websites and Applications." If not accurate, explain any deviation from appropriate Privacy Notice and/or OMB M-10-23.

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.

Explain the standards and relevant controls that the CFPB – or any third-party contractor – must meet in order to collect, use, disclose, or retain information. For standards relevant to the CFPB, explain how the CFPB manages risks to privacy by complying with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002; voluntarily adopting Office of Management and Budget privacy-related guidance as best practice[1]; and applying National Institute of Standards and Technology risk management processes for privacy.

PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA. Address whether information has been stripped of direct identifiers prior to direct access or prior to use by CFPB employees; whether data fields are masked for different users, etc.

Explain how the information will be secured. List the relevant technical and administrative controls and describe their uses.

"The CFPB uses the following technical and administrative controls to secure the data and create accountability for the Bureau's appropriate collection, use, disclosure, and retention of the information:

- Audit Logs and Reviews
- CFPB Personnel Privacy Training
- CFPB Privacy Incident Response and Recovery Plan
- Compliance with CFPB cybersecurity policy and procedures
- Data Quality and Integrity Checks
- Extract logging and 90-day reviews
- Policy and Standard Operating Procedures
- Role-based Access Controls: [describe]

[1] Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with Office of Management and Budget (OMB)-issued privacy guidance, its intention is to voluntarily follow OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

- Federal Committee on Statistical Methodology Government-wide Statistical Standards
- Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies
- Records Schedule Submitted to/Approved by National Archives and Records Administration: [list]"
- Personnel Security including background checks

Discuss the role of third-party contractors acting on behalf of the CFPB, if any. As appropriate, explain what role contractors play in collecting, aggregating, or stripping direct identifying information. Select the relevant technical and administrative controls used to protect against inappropriate collection, use, disclosure, retention and/or disposal of information. Describe any relevant contract provisions.

For Agile development, system CRs, and SA&A packages, address Agile/CR/SA&A Checklist, discuss the type of IT environment used, e.g. testing or production environment; whether synthetic or otherwise modified operational information was used; and whether any fields or information were masked or truncated to reduce the sensitivity of the information.

Explain compliance with CFPB web measurement and customization technologies requirements

Discuss the disclosure avoidance technique(s) and standard(s) (if any) used for this data and why. Some possible techniques include:

- record swapping
- blanking and imputation
- rank swapping
- random noise
- cell suppression
- controlled rounding

- generation of synthetic data (include information on which variables were synthesized, which were not, which were used in the model, and the percent of records that were synthesized)
- publish sub-samples
- eliminate geographic inferences

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.)

Describe any due diligence used to select third party (ies) that collaborate or partner with the CFPB. Explain the standards that the CFPB or any third party collaborator(s) or partner(s) must meet in order to collect, use, disclose, or retain information. For example, standards relevant to third parties may include compliance with Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, or the Right to Financial Privacy Act. Standards may also include applicable privacy policies or data release forms.

Document control

Approval

_____

Chief Information Officer

Date

_____

Chief Privacy Officer

Date

_____

Name

Initiative Owner

Date

Change control

Version	Summary of material changes	Pages affected	Date of change
