[DATE]

Privacy Impact Assessment

[SYSTEM NAME]

Contact Point:
Claire Stapleton
Chief Privacy Officer
1700 G St, NW
Washington, DC 20006
202-435-7220
claire.stapleton@cfpb.gov

Note

This document represents the CFPB's template for conducting Privacy Impact Assessments (PIAs). While published PIAs may differ from this document in terms of visual style and presentation (e.g., colors, formatting, typefaces, etc.), all CFPB PIAs are conducted substantively in accordance with the framework presented on the following pages.

Document purpose

The Privacy Impact Assessment, or "PIA", provides the public with information about the Consumer Financial Protection Bureau's ("CFPB") collection and use of personally identifiable information ("PII"). PII is any information "that can be used to distinguish or trace an individual's identity" like a name, address, Social Security number, or place and date of birth. The CFPB uses PIAs to document that 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:

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 or other identifier
❑ Financial Information
❑ User and Online Information
❑ Third Party Information
❑ Other Information (including biometric information and health or medical information)

The overview is a short description of the project. The overview should include no less than:

- Descriptions of the purpose of the project – why this system, technology, pilot, rule, program, or other collection ("project") is being completed, what legislation authorizes it, and how it relates to the CFPB's mission of protecting American consumers;

- Descriptions of what PII is collected and who it is collected from;

- Descriptions of how the project collects and uses PII, including an example that illustrates what happens to the PII from the time it is collected until it is destroyed;

- If applicable, reference any associated SORNs by Federal Register citation in the overview. You may later reference associated SORNs by the CFPB name and number only.

SECTION 1.0

Purpose of collection

The CFPB will state the purpose and legal authority for collecting personally identifiable information ("PII").

1.1 Why is the information being collected?

Include a statement of why the PII is being collected and why collecting it is necessary in carrying out the program's mission or goal. This should align with the Purpose section of the relevant System of Records Notice ("SORN"). A general statement about the purpose without discussing particular PII is not an adequate response.

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

List all statutory and regulatory authorities, as well as any Executive Orders, that authorize the collection, maintenance, use, and dissemination of the PII to meet the program mission or goal. Also include any Memoranda of Understanding ("MOUs") that authorize the collection, maintenance, use, and dissemination of the PII.

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?

For all collections of PII where the information is retrieved by a personal identifier, the Privacy Act of 1974 requires that the agency publish a SORN in the Federal Register. Include the CFPB number (CFPB - X) for the SORN. If no SORN is required, explain why not (e.g., either a program specific or government-wide SORN already covers the collected information or information is not retrieved by a personal identifier).

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.

If an approved NARA records schedule exists, please provide the records schedule number (XX-587-XX-XXX) and explain for how long and for what reason the information is retained. If a general records schedule ("GRS") covers the information, then please provide the GRS number (GRS X, Item X) and explain for how long and for what reason the information is retained.

If there is not an approved NARA records schedule or GRS, then the project manager should consult with the records management officer to develop a records retention schedule for the records contained in the system for the minimum amount of time necessary to fulfill the needs of the project. If a NARA-

approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule. If a proposed records schedule is pending approval with NARA, then please provide the NARA job number (XX-587-XX-XXX), if known.

If CFPB has contracted with an outside party to manage our records for the project, then validate that the retention and disposal procedures are outlined in the contract. This scenario may include when the outside party only manages partial records in the system. In addition, discuss how the records will be maintained during the project and how they will be disposed of after the completion of the project.

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")?

If the information is covered by the PRA, provide the Office of Management and Budget ("OMB") Control Number and the CFPB control number for the collection. Attach a copy of the form, a screenshot of or link to the web form, or the survey as an appendix to the PIA. If there are multiple forms or surveys, attach a copy of the forms or surveys in the appendix and include a list in the response to this question within the PIA.

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?

Discuss any privacy risks associated with the purpose of the collection of the information in the project. For example, are all the purpose(s) for which the information may be used specified at the time of collection? If not, why not? If information may later be used for reasons other than the purpose specified, will individuals have the opportunity to consent to the new use? Discuss how any associated risks are mitigated. If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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.

In many cases, agencies provide written or oral notice before they collect information from individuals. For the CFPB, that notice may include a posted privacy policy, a Privacy Act Statement on forms or on a survey, a PIA, a SORN published in the Federal Register, or information provided on the CFPB website. Describe what notice was provided to the individuals whose information is being collected. If notice was

provided in the Federal Register, provide the citation (XX FR XXXX, Date) and any associated CFPB number.

If notice was provided by a Privacy Act Statement, please describe the content of that notice and attach a copy as an appendix. Describe how the notice provided for collection of information is adequate to inform those who are impacted by the collection.

If notice was not provided, explain why. For example, notice may not be appropriate for certain law enforcement projects. If this is the case, you should explain why providing notice would undermine the law enforcement mission.

If the information is collected from someone other than the individual explain how that information is collected and how the individual was provided notice of the use of the information being collected.

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

In many cases, agencies provide written or oral notice before they share information about individuals. For the CFPB, that notice may include a posted privacy policy, a Privacy Act Statement on forms, or a survey, a PIA, a SORN published in the Federal Register, or information provided on the CFPB website. Describe what notice was provided to the individuals to inform them that the collected information may be shared. If notice was provided in the Federal Register, provide the citation (XX FR XXXX, Date).

If notice was provided by a Privacy Act Statement, describe the content of the notice and attach a copy as an appendix. Describe how the notice provided for sharing the collected information is adequate to inform those who are impacted by the collection.

If notice was not provided, explain why. For example, for certain law enforcement projects, notice may not be appropriate. If this is the case, explain why providing notice would undermine the law enforcement efforts.

If the information is collected from someone other than the individual explain why that information is being collected from another source and how the individual was provided notice.

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?

Discuss any privacy risks posed by this system or information collection with regard to openness, and transparency. For example, if notice is only provided through the publishing of this Privacy Impact Assessment, discuss the reasons for limited notice and any impacts that may pose to the privacy of affected individuals. Discuss how any associated risks are mitigated. If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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 fulfill that purpose.

3.1 Whose information is included in the system?

List all of the individuals who will be covered by the system. For example, employees, contractors, and those individuals who filed a complaint or made an inquiry, etc.

3.2 What PII will the system include?

List all PII that is going to be collected including but not limited to: name, date of birth, mailing address, telephone number, Social Security number ("SSN"), email address, bank account number, etc. In particular, your answer should focus on PII collected about and from the public, but should not neglect information collected on CFPB employees and contractors. Information should be considered to be "collected" even if it comes to the CFPB through an information sharing activity or via a hotline or other similar medium. The answer to this question should align with the information provided for the annual PII Inventory.

If SSNs will be collected, state why the SSN is necessary and how it will be used. Discuss why the SSN is the best identifier for this system. In your discussion, explain whether you considered using only the last four digits of the SSN. If you concluded that the last four digits were insufficient, explain why. Also include what safeguards are in place to minimize any privacy incident.

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

Include a statement of why the collection of PII is necessary to achieve the project mission. For example, a statement that the system may collect name, date of birth, and biometrics in order to identify those individuals who enter the CFPB premises is adequate. However, merely stating that the above data will be collected to verify identity is insufficient.

When answering the question, explain why the collection of non-PII will not work for the project.

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?

Modernized systems often have the capability to derive new data and create previously unavailable data about an individual through aggregation from the information collected. The "mosaic theory" is the idea that disparate pieces of information, though individually of limited or no value, can be significant when combined with other pieces of information that could result in an unforeseen vulnerability, exploitation or misuse of the information.

What is meant by the terms "derived" and "aggregation"?

Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information.

Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data, i.e., tables or data arrays, that is usually different from the source information.

Discuss whether the system will aggregate or derive data. In addition, discuss how this information will be maintained and used.

If any new data that may be considered PII will be generated by the system, include those fields. For example, a unique identifier may be generated by the system and provided to the user for future follow up.

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

Explain the controls, including how they are sufficient and how the decision was made to move forward with the selected controls.

If the data is being consolidated (combined or consolidated into one system, application or process), then the existing controls should protect the data. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III at http://www.whitehouse.gov/omb/circulars/a130/appendix_iii.pdf.

3.6 Will the system monitor the public?

Most modernized systems have the capability to identify, locate and monitor individuals. Because we are a consumer agency, monitoring of the public should be at a minimum and only that necessary to carry out the purpose of the system. This is important in order to maintain the public's trust. Discuss whether the system will monitor the public and for what purpose. If a monitoring capability does exist and will be used, please discuss why the capability is necessary and how it will be used. Include how the decision was made to move forward with a monitoring capability and what safeguards are in place to reduce impact on personal privacy.

3.7 Will the system monitor employees or contractors?

Discuss whether the system will have a monitoring capability and the purpose for the monitoring. Discuss whether someone will review the logs created by the monitoring. Discuss any safeguards to prevent abuse.

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

List the types of reports that will be produced and discuss the use for the reports. In addition, discuss whether the report will produce anonymized data. If data will not be anonymized, discuss why. Include those offices that will have access to the reports.

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

Discuss any privacy risks associated with data minimization with the system. For example, explain whether any data collected that is not necessary for the stated purpose. If so, discuss why the data is collected and whether or not individuals have the ability to decline to provide this information. Discuss how any associated risks are mitigated. If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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?

The project should collect PII only for specific, explicit, and legitimate purposes and used in a way that is compatible with those purposes. Discuss how the information collected is limited to the purpose for which the PII was collected. Also, discuss how the CFPB will ensure that the information collected will only be used in ways that are compatible with the purpose for which the PII was collected. This information should align with the compatibility statements from the Report to Congress/OMB.

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?

Discuss the external CFPB sharing of information, e.g., the CFPB to the Federal Reserve Board of Governors. Identify the name or names of other individuals, Federal, state and local agencies, and private sector organizations with which the CFPB may share information.

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

If the information is being collected from sources other than the individual, including other IT systems, system of records, commercial data aggregators, and/or other Federal, state or local agencies, state the sources of the information and why taking the information from other sources is required.

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

Describe what systems the CFPB system will interact with, either within or outside of the CFPB. Describe how the data is transmitted. For example, is the data transmitted electronically, in bulk, by paper, direct access, or by some other means? Discuss whether access controls have been implemented to ensure appropriate sharing of information. State whether there is a ("MOU"), contract or agreement in place and define the parameters of the sharing agreement.

If data is being shared externally, discuss whether the receiving system has undergone a Security Certification & Accreditation ("C&A"). For sharing with non-Federal agencies, discuss how the relevant privacy protections have been expressed and documented to ensure the privacy and security of the information once it is shared. If necessary, discuss the provisions for notification of a suspected or confirmed privacy incident.

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

Discuss the privacy risks associated with the sharing of information outside of the CFPB. For example, if information is disclosed or shared with other federal agencies, are individuals made aware of such sharing and how shared data will be used or secured? If not, why? Discuss how any associated risks are mitigated. If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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?

Discuss whether the source of the data is from the project itself or whether it comes from the individual directly or some other source. Describe any technical solutions, policies, or procedures focused on data accuracy and integrity of the project.

If the data comes from some other source, explain how the CFPB will ensure its accuracy and completeness.

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?

Discuss the privacy risks associated with data quality and integrity of the project. How are these risks mitigated? If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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?

List those individuals who will have access to the data in the project and state their respective roles. Individuals may include, for example, contractors, managers, program staff, and developers (e.g., program staff will have access to review complaints, contact the complainant and process the complaint).

Describe the process and authorization for access to the project for each user. Also describe the processes and policies surrounding termination of access to the project for each user when access by that user is no longer needed.

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

Provide the date that the authority to operate the project was granted or is expected to be granted. For a new project, state the date of the Certification & Accreditation (C&A) completion . If a C&A is not required, state that along with an explanation.

6.3 How will the system be secured?

Indicate any physical controls that will be implemented (security guards, identification badges, key cards, safes, locks, etc).

Indicate any technical controls that will be implemented (user identification, password, intrusion detection, encryption firewall, etc).

List any administrative controls that will be implemented (periodic security audits, regular monitoring of users, backup of sensitive data, etc).

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

Discuss what security incident reporting plan and procedures are in place to effectively handle a security incident involving the system.

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

Discuss the privacy risks associated with security for this system. How are these risks mitigated? If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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.

State whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. State how the consent is given. If the individual can decline or opt out, how is this done?

7.2 What procedures will allow individuals to access their information?

Describe any procedures or regulations allowing an individual access to information collected by the system and/or the accounting of disclosures of that information. These procedures should include the CFPB's Freedom of Information Act ("FOIA") and/or Privacy Act practices. If an individual cannot access their information through the FOIA/Privacy Act process, state why.

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

Discuss the procedures for an individual to address possibly inaccurate or erroneous information about him/her. These procedures should include the CFPB's FOIA/Privacy Act practices. If an individual cannot access their information through the FOIA/Privacy Act process, state why.

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

Discuss the privacy risks associated with individual participation with the system. How are these risks mitigated? If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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 privacy and security training. However, each project may also offer specific training on information handling procedures and sensitivity of information. Discuss how individuals with access to PII are trained to appropriately handle the PII. Explain what controls are in place to ensure that users of the system have been trained and that the training is documented.

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?

Discuss the privacy risks associated with awareness and training with the system. How are these risks mitigated? If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.

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?

Discuss auditing measures as well as technical and policy safeguards such as information sharing protocols, special access restrictions and other controls (for example, "read-only" access capability). Explain whether the system will conduct the audits or whether third parties, such as the Office of the Inspector General or the Government Accountability Office, will conduct reviews.

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?

Discuss the privacy risks associated with accountability and auditing for this system. How are these risks mitigated? If alternatives were considered, include information on how the decision was made to move forward with the selected alternative.