

JANUARY 4, 2012

Privacy Impact Assessment

FREEDOM OF INFORMATION ACT AND PRIVACY ACT SYSTEM



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

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”¹ 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:

Freedom of Information Act and Privacy Act Request System

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 Dodd-Frank Wall Street Reform and Consumer Protection Act (the “Act”), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau (the “CFPB”). The CFPB administers, enforces, and implements federal consumer financial protection laws, and among other powers, has authority to protect consumers from unfair, deceptive, and abusive practices in consumer financial products or services.

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 his or her 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.”

The CFPB Freedom of Information Act (“FOIA”) and Privacy Act System will be used by the CFPB to collect, process, log, track, and respond to all FOIA and/or Privacy Act related requests submitted to us or to other agencies when the requested information relates to the CFPB. An individual submitting a FOIA and/or Privacy Act request to the CFPB provide PII that varies depending on the request, but that generally includes name and contact information. The system of records notice for the CFPB.001 CFPB Freedom of Information Act (“FOIA”) / Privacy Act System was published at 76 FR 45767.

The CFPB will be using an electronic FOIA and Privacy Act Request System. This is a comprehensive application that can process both FOIA and Privacy Act requests. The application includes:

- Request Management
- Correspondence Management
- Document Management
- Fee/Payment Management
- Document Redaction, Review and De-Classification
- Reporting

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?

The CFPB uses information in the system to process requests for records and administrative appeals under FOIA, as well as access, notification, and amendment requests and appeals under the Privacy Act.

For a FOIA request, we will collect the requester’s name, address, phone number, and email address to allow us to correspond with the requester. If requests require PII to locate potentially responsive records, that information will be collected. Otherwise we will not collect PII other than contact information.

For a Privacy Act request, we may need to locate the records using a name or unique identifier. We will collect the minimum amount of PII required to locate potentially responsive records, and to correspond about the request. A Privacy Act request requires that the requester also provide two forms of identification, one that includes a photograph and one that bears the signature of the requester.

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

The Freedom of Information Act of 1996, as amended 5 U.S.C. § 552; Privacy Act of 1974, as amended 5 U.S.C. § 552a; Pub. L No. 111-203, Title X of the Consumer Financial Protection Act, Section 1066, codified at 12 U.S.C. § 5586. The Presidential Memorandum for Heads of Executive Departments and Agencies Concerning the Freedom of Information Act, 74 Fed Reg 4683 and the OMB Director’s Open

Government Directive Memorandum, dated December 8, 2009, provide guidance on disclosure for government agencies to ensure openness and transparency in all government agencies.

- 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, information in the system is searchable by personal identifier. The CFPB has given notice of this system of records under CFPB.001 – Consumer Financial Protection Bureau FOIA/Privacy Act.

Records can be retrieved by a variety of fields, including:

- Requester's name
- Requester's address
- Requester's phone number
- Requester's email address and/or fax number (optional)
- Description of request
- FOIA request number
- Staff member assigned to process the request

The information can also be retrieved by any combination of these fields.

- 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.

Yes. The CFPB will maintain electronic and paper records in accordance with published National Archives and Records Administration Disposition Schedule, Transmittal No. 22, General Records Schedule 14, Information Service Records. Records pertaining to FOIA and Privacy Act programs are retained and disposed of in accordance with the GRS 14. The retention schedule is brief enough to ensure privacy protection, but long enough to ensure the operational integrity of the FOIA/Privacy Act program.

- 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”)?

The eFOIA system will use an online intake form for the collection of information that would be covered by the PRA. The online intake form requires that the requester complete the form to submit a request. OMB has granted an exemption for FOIA forms that only include contact information in order to respond to the request for information.

- 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?

There are no risks with this system that relate to the purpose of collection.

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.

This PIA and the associated System of Records Notice (“SORN”), CFPB.001–Freedom of Information Act/Privacy Act, provide constructive notice of the CFPB’s information collection practices .

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

The CFPB has provided notice of how information stored in the eFOIA system may be disclosed or shared in its SORN, CFPB.001 – Freedom of Information Act/Privacy Act.

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?

No, there are no risks to openness and transparency when submitting either a FOIA or Privacy Act request. The CFPB uses the FOIA process in its efforts to provide transparency on the CFPB’s activities

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?

The FOIA and Privacy Act Request System contain information on individuals who request access to records under FOIA or Privacy Act. Other individuals include the CFPB staff assigned to process the requests, and employees who may have responsive records or are identified in the records.

3.2 What PII will the system include?

Information from individuals may include:

- Requester’s Name

- Requester's Address
- Requester's phone number
- Requester's email address and/or fax number (optional)
- FOIA request number
- Information identifying the entity that is subject to the request or appeal
- Privacy Act requests may also contain Social Security numbers if submitted with documentation or as proof of identification and date of birth

The system may also contain correspondence with the requester including:

- Initial requests, acknowledgement letters, interim as well as final responses, and appeals
- Documents generated or compiled during the search and processing of the request
- Fee estimates and fee calculations
- Comparable records with respect to any appeals made from initial denials of access, refusals to amend records, and lawsuits under FOIA and Privacy Act
- Documents and memoranda to support the decision made in response to the request, referrals, and copies of records provided or withheld
- Legal memoranda and opinions
- Information relating to the Bureau staff assigned to process, consider, and respond to requests

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

The CFPB requires contact information about requesters in order to process and respond to FOIA and Privacy Act requests.

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?

The system will not aggregate or create new data about individuals.

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

The system will not aggregate, consolidate, or create new data about individuals.

3.6 Will the system monitor the public?

The system will not monitor the public.

3.7 Will the system monitor employees or contractors?

Yes. The program will track which CFPB employees are involved in or responsible for responding to FOIA and Privacy Act requests. Such monitoring will be used to facilitate responses to FOIA and Privacy Act requests and appeals, to improve processing workflows, to ensure quality, to provide security, and to facilitate audits of the program.

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

The FOIA and Privacy Act require Federal agencies to provide statistical reports about their FOIA and Privacy Act compliance efforts to the Department of Justice and the Congress. None of these reports require or seek information about individual FOIA requesters and the Bureau will provide no such information.

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

Information in the FOIA and Privacy Act Request System is limited to information gathered or used in the course of responding to, tracking, or otherwise managing FOIA/Privacy Act requests.

The CFPB requires limited contact information from the requester. This includes name, address, phone number, email address, fax number, FOIA request number, or some combination of these data elements. If the requester provides other personal information, the CFPB will not enter the extraneous information into the FOIA and Privacy Act Request System although the original request will be retained.

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 PII contained in the FOIA and Privacy Act Request System is limited to contact information and the information required to fulfill the request.

- 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?

Pursuant to the CFPB's regulations, 12 C.F.R. § 1070.10 et seq., the CFPB may share FOIA or Privacy Act requests with other Federal Government agencies to the extent that the requests concern records or information that belong to or originate with those agencies and the input of those agencies is necessary to determine an appropriate response to the requests. Likewise, the CFPB may share FOIA or Privacy Act requests with businesses to the extent that the requests concern records of those businesses and the input

of the businesses is necessary to determine an appropriate response to the requests. The CFPB documents other ways in which the information for this program may be shared under its “Routine Uses” section of the SORN.

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

Individual requesters provide their information directly to the CFPB when initiating a FOIA or Privacy Act request.

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

The eFOIA system will interact with Consumerfinance.gov to allow requesters to file, check the status of or see results of their request, or to make records available to the public.

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

There are minimal risks associated with use limitation for this system. The CFPB limits access to the FOIA system to CFPB employees whose duties require them to have access to the system. The CFPB provides all employees with privacy and security training.

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?

We do not verify information individuals provide through FOIA for accuracy or completeness. The information requested comes directly from the individual, so we assume that the information is correct. We will not attempt to verify your identity as the submitter when submitting a FOIA request. However, verification of ID is required for Privacy Act requests as outlined in 12 C.F.R. 1070 *et seq.*

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?

FOIA and Privacy Act requesters are responsible for submitting or inputting directly most of the information contained within this system of records. There is a risk that the information that these requesters submit or input is incorrect, erroneous, or obsolete.

For Privacy Act requests, the CFPB mitigates this risk, in part, by validating the information submitted. The CFPB's Privacy Act regulations require requesters to submit two forms of identification together with their request –one that includes a photograph and one that bears the signature of the requester. If the identity of the requester cannot be verified, then the CFPB will not process the request.

At any time, the requester may contact the CFPB to correct or update any information they submit to the CFPB in connection with a FOIA or Privacy Act request.

In addition, the CFPB also provides a means through the Privacy Act of amending or correcting any records that the CFPB maintains about an individual at that individual's request.

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?

Access to the FOIA and Privacy Act Request System will be limited to individuals whose job functions include FOIA/Privacy Act related duties. Additionally, the CFPB may grant contractors acting on behalf of the CFPB access to the system and its information.

Access is restricted to authorized personnel who have been issued non-transferrable access codes and passwords. The CFPB may also maintain information in locked file cabinets or rooms with access limited to those personnel whose official duties require access.

Contractors and employees who no longer have a defined business need to access the information – either by a change in job function, termination or resignation – will have their access removed.

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

The CFPB is currently developing a system security plan (“SSP”) for the eFOIA system under the General Support System (“GSS”). The SSP will be approved prior to the deployment of the eFOIA program. The GSS system's Authority to Operate (“ATO”) at the Moderate level was signed on September 30, 2011.

6.3 How will the system be secured?

The CFPB issues authorized personnel, including employees and contractors acting on behalf of the CFPB, non-transferrable access codes and passwords to the system. The CFPB may also maintain

information in locked file cabinets or rooms with access limited to those personnel whose official duties require access. Access is limited to those with a CFPB issued username and password.

Standard operating procedures exist for terminating or reducing access for individuals who no longer have a need to know all or certain information contained in the FOIA and Privacy Act Request System.

The CFPB has implemented extensive security controls and safeguards for the FOIA and Privacy Act Request System to protect information contained in the system against unauthorized disclosure and access. These include:

- CFPB policies and procedures governing privacy and information security;
- Conducting background checks on all personnel with access to the system;
- Initial and follow-on privacy and security awareness training for each individual with access to the system;
- Physical and technical perimeter security safeguards;
- Security Operations Center to monitor antivirus and intrusion detection software;
- Risk and controls assessments and mitigation; and
- Technical and physical access controls, such as role-based access management and firewalls.

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

Since the CFPB is currently using elements of Treasury's network, the CFPB relies on Treasury's directives that relate to security and privacy incidents. The CFPB is developing supplemental interim incident-reporting materials. When the CFPB moves onto our own network infrastructure, will issue new directives related to security and privacy incidents.

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

There is a risk that unauthorized individuals may gain access to the information in the FOIA and Privacy Act Request System. The CFPB has mitigated this risk by granting access to the system to authorized users, based on their need to know, and will be restricted to the amount of data required or appropriate to carry out their assigned job responsibilities. Access is terminated or reduced if the employee or contractor no longer have a need to know the information, change jobs, terminate or resign.

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.

The CFPB requires certain information about a FOIA or Privacy Act requester in order to process requests for CFPB records. An individual may choose not to provide this information, but if he or she does not do so, the CFPB may not be able to process their FOIA or Privacy Act request.

- 7.2 What procedures will allow individuals to access their information?

The CFPB provides a means through the Privacy Act of amending or correcting an individual's records at their request or the request of their Congressional representative, with the written consent of the requester. Information about FOIA/Privacy Act requests are available in the CFPB Freedom of Information Act / Privacy Act System of Records Notice and on the CFPB website at <http://www.consumerfinance.gov/foia>.

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

See answer to 7.2

- 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 an individuals' information may be released without their knowledge or consent.

When an individual submits a FOIA request, the nature of the request and the identity of the requester becomes publicly available information. For example, a member of the public may file a FOIA request that seeks copies of all FOIA requests filed by a particular individual or that relate to a particular topic. Furthermore, the CFPB summarizes and publishes information about the FOIA requests it receives.

The CFPB does not release to the public the identities of individuals who file Privacy Act requests.

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 to all employees of the Bureau, including contractors who handle PII on behalf of the CFPB.

- 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?

There are no risks that relate to awareness and training.

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 CFBP provides employees and contractors with base-level training relative to data privacy and security.

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?

The FOIA and Privacy Act Request System has built in auditing controls. The auditing controls will show all actions taken by a user on any case. This auditing feature maintains accountability of an action taken by an authorized user. Paper-based systems are monitored, managed, and audited by the FOIA Manager.