

DECEMBER 15, 2011

Privacy Impact Assessment

CONSUMER RESPONSE SYSTEM



Consumer Financial
Protection Bureau

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:

Consumer Response 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, Public Law No. 111-203, Title X, established the CFPB. The CFPB administers, enforces, and implements federal consumer financial law, 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 CRS collects, responds to, and refers consumer contacts about consumer financial products, services and entities. These contacts may include complaints, inquiries, or comments about consumer financial products, services, the entities providing them, or about the CFPB. For the purposes of the CRS and this PIA, the CFPB refers to all of these as “contacts.” The CRS will not collect correspondence not related to consumer contacts.

In order to help resolve and refer consumer contacts, the CRS collects and uses PII, including information about individuals who submit contacts to the CFPB; individuals who have contacts submitted on their behalf; and individuals who are the subject of contacts that the CFPB receives.

The CFPB’s website ConsumerFinance.gov provides several ways for consumers to get information about or discuss financial products, services, and entities, or to submit a contact to the Bureau. These include a moderated discussion forum, Frequently Asked Questions (“FAQs”), “Tell Your Story,” and the online complaint submission form (https://help.consumerfinance.gov/app/ask_cc_complaint).

You can also submit a complaint about a financial product or service by calling a toll free number or by requesting and mailing back a completed form.

COMPLAINTS BY WEB-FORM

When you submit a complaint through the form on ConsumerFinance.gov, you provide some contact information, information regarding the financial product or service you are complaining about, your experience, and responses to a short series of questions. You can review your complaint and make any necessary edits to your complaint before submitting it to the CFPB. The CFPB will send you an e-mail or letter confirming the receipt of your complaint. The CFPB then reviews the complaint and, if appropriate, directly relays it to the entity providing the financial product or service. The entity can review the complaint and is responsible for responding directly to the CFPB with a resolution. The entity may also respond directly to you.

COMPLAINTS SUBMITTED BY MAIL OR FAX

You may also mail or fax complaint forms to the contact center. A customer service representative scans the form (with optical character recognition) and uploads it into the CRS. The CFPB will send you an e-mail or letter confirming the receipt of your complaint. The CFPB then reviews the complaint and, if appropriate, directly relays it to the entity providing the financial product or service. The entity can review the complaint and is responsible for responding directly to the CFPB with a resolution. The entity may also respond directly to you.

Physical copies of faxes or mail the CFPB receives are stored in locked file cabinets until they are destroyed under an applicable records schedule. The CFPB similarly uploads faxes it receives through 1-855-CFPB-FAX into the CRS, with physical copies stored in locked file cabinets until the Bureau destroys them under an applicable records schedule.

CONTACTS SUBMITTED BY TELEPHONE

You may call the contact center via the consumer response toll free telephone number, 1-855-411-CFPB. Customer service representatives enter the relevant information from these telephone calls into the CRS. Following industry standard quality assurance processes, the CFPB records these calls and your customer

service representative informs you that the call is being monitored for quality assurance. The CFPB will send you an e-mail or letter confirming the receipt of your complaint. The CFPB then reviews the complaint and, if appropriate, directly relays it to the entity providing the financial product or service. The entity can review the complaint and is responsible for responding directly to the CFPB with a resolution. The entity may also respond directly to you.

Some complaints, whether submitted by Web-Form, Mail, Fax or Telephone, may warrant further investigation by the CFPB. Investigation entails working with the entity, potentially collecting additional information from the entity or you, and conducting additional analysis. Investigators log cases and, if necessary, flag them for inclusion in supervision and enforcement databases.

WHISTLEBLOWER CONTACTS

Employees of financial institutions and other with knowledge of their practices may anonymously submit a contact through any of the above methods. These contacts are logged in the CRS but access to them is restricted to Investigations Managers and Enforcement Attorneys who research the validity of the contacts and take appropriate further action. Unlike consumer complaints, whistleblower contacts are not made available to financial institutions.

OTHER SUBMITTED CONTACTS

There are other features on ConsumerFinance.gov in addition to the complaint submission form. You can view questions and discussions about financial products and services in the moderated discussion forum, as well as the FAQs. You may also take advantage of the “Tell Your Story” feature, which allows you to share your experience with a financial product, service, or the CFPB.

You can view FAQs and discussion forum threads without providing any of your PII. You can use the “Tell Your Story” feature by providing an email address when you submit your story. The CFPB only requires this field so that it can contact you to gather more information if necessary for investigative purposes. You may choose to submit more PII in the additional contact fields but can submit a story without doing so.

If you want to post to the moderated forum discussion or respond to a posted question, you are required to create a user account with minimal PII such as your name and an e-mail address. This account also allows you to log in and check the status of any complaints you have submitted, and to see a history of any questions you posted to the forum. The CFPB removes questions containing PII or personal financial information from the discussion forums. If you post to a discussion thread and we remove your post, we try to tell you why and give you a chance to submit a revised post.

The CFPB also provides you an opportunity to get answers to more general questions without going through the complaint process. General questions and standard CFPB responses are available at ConsumerFinance.gov.

The CRS stores contacts related to financial products, services, or entities as individual cases that are attached to individual consumer profiles or accounts where appropriate. You have the ability to add a password to your login information (your submitted e-mail address) so that you can periodically check the status of your complaint.

The CRS is documented in a System of Records Notice (“SORN”); CFPB.005 –Consumer Response System [76 FR 68396]. The CFPB previously gave notice of this system under Treasury/DO.315 – CFPB Implementation Team Consumer Inquiry and Complaint Database [76 FR 1507].

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 the PII it collects through the CRS to respond to and refer consumer contacts about consumer financial products, services and entities.

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

The Dodd-Frank Wall Street Reform and Consumer Protection Act (“Act”), Public Law No. 111-203, Title X grants the CFPB authority to operate the CRS. Specifically, Pub. L. No. 111-203, Title X, Sections 1011, 1012, 1013(b)(3), 1021, 1034 codified at 12 U.S.C. §§ 5491, 5492, 5493(b)(3), 5511, 5534.

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?

Information in the CRS is searchable by PII, including:

- Name;
- Complaint/inquiry case number;
- Address;
- Account number;
- Transaction number;
- Phone number; and
- Date of birth.²

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 maintains computer and paper records indefinitely until NARA approves the CFPB’s records disposition schedule. Records that fall under a general records schedule will be disposed of according to the applicable schedule.

² The system can also retrieve records by any combination of these fields. This list is not exhaustive.

- 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 CFPB uses a form to collect information for the CRS. A list of the associated form(s) covered by the PRA, including Office of Management and Budget (“OMB”) Control Numbers and approval dates is available in Appendix A.

The CRS also collects information through phone calls to the CFPB’s consumer response toll free number (1-855-411-CFPB). The information collected through the telephone is similar to the information collected through the form.

- 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. There are no risks associated with the purpose of collection for the CRS.

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.

The CFPB provides notice to you if you choose to submit a contact. You can limit the amount of PII you disclose to the CFPB or you can make an anonymous complaint. Additionally, the CFPB notifies you that we are collecting your information when you submit a complaint via telephone, and advises you that the call may be monitored and recorded.

The CFPB has provided notice for those who work at an entity that is the subject of a complaint through this PIA and the CRS SORN. For example, when consumers contact the CFPB to make a complaint, the consumer may include information about employees at the entity providing the financial product or service.

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

The CFPB provides notice regarding the sharing of your information as it pertains to a contact you submit to the CFPB. The CFPB has documented all of the ways in which it may disclose the information contained in the CRS in its SORN, CFPB.005 –Consumer Response System.

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 for CRS that relate to openness and transparency.

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 CRS includes information about individuals who submit contacts to the CFPB; who have contacts submitted on their behalf; and individuals at entities about which contacts have been received.

3.2 What PII will the system include?

The CRS contains information derived from contacts from consumers. The information in the system may vary based on the information provided by those who submit the contact, but may include:

- Name;
- SSN;
- Account, loan and client numbers;
- Contact information such as address, e-mail, phone, or fax number;
- Limited demographic information (related to individuals who self-identify as victims of discrimination or as current or former members of the military); and
- Age and date of birth.

Although the CFPB does not request SSNs for all contacts, some individuals may choose to provide their SSN in a complaint. In some cases, the CFPB may request your SSN to validate your identity and for association with a particular account you are complaining about (for example, credit reports). Rather than encourage individuals to enter truncated SSNs, the CFPB has opted to allow individuals to choose how much information they share when making a complaint

In some cases, the CFPB will delete certain sensitive information, such as SSNs and some types of account numbers from the CRS when the CFPB no longer needs the information to process the complaint. This further enhances your privacy and the security of the CRS.

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

The collection of PII is necessary to enable the CFPB to respond to those who request a response about their complaint. The CFPB uses the information provided in a contact to resolve or refer that contact as appropriate, and to inform other functions of the CFPB.

- 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 does not aggregate or create new data about individuals.

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

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

- 3.6 Will the system monitor the public?

The system does not monitor the public.

- 3.7 Will the system monitor employees or contractors?

The system allows for the monitoring of employees or contractors acting on behalf of the CFPB. This function exists for the purpose of tracking cases for resolution, workflow improvements, quality assurance, and security and auditing capabilities.

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

The CFPB may generate reports from the CRS in order to respond to or refer contacts, or in order to inform other functions of the Bureau. The CFPB may also create reports as necessary to inform other agencies, as required by law. This could include a list of names and contact information of individuals who submitted complaints or inquiries for follow-up. Another example would be a list of consumers who are customers of an institution who have all filed similar complaints about a particular financial product. The CFPB may produce reports of anonymized aggregate data about trends in complaints or inquiries received by the Bureau. Similarly, the Bureau may also create reports that allow it to meet its mission and statutory mandates.

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

There is a risk that individuals who submit a contact could provide more information than is necessary to resolve or respond to the inquiry or complaint. To help mitigate that risk, the CFPB created a web form that directs individuals to submit only that information which is necessary to resolve or refer their contact. The CFPB provides security and privacy training to its customer service representatives who collect complaints or inquiries via the telephone, and provides scripts that direct callers to provide only that information which is relevant to the subject of their call.

A privacy statement on the intake form outlines the reason for the collection of information and how the information is used. Individuals are encouraged not to submit PII when using “Tell Your Story” features and the discussion forums.

There is also a risk that individuals could unnecessarily provide their SSN. Though the CFPB does not request SSNs for most contacts, individuals may choose to provide their SSN during the process of submitting a contact, and in some cases, the CFPB may request an SSN to resolve a complaint when the entity that is the subject of the complaint uses that number as a way to identify an account. The CFPB has built-in processes and controls to limit the chance of a SSN being included when it is not necessary. Trained customer service representatives guide individuals who choose to submit complaints or inquiries via telephone on what information to provide when making a complaint.

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?

Some information provided to the CFPB by consumers and financial institutions during the inquiry or complaint process may include unnecessary PII about customers or employees of the institution. Section 3.9 discusses this risk and the CFPB’s strategy for mitigating it.

- 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?

Yes, in many cases, the CFPB shares the information it receives with the appropriate third parties necessary to resolve or respond to a complaint. This may include information about the consumer financial product, service, or entity.

In some circumstances, the CFPB may share the PII you provide with third parties such as other federal regulators or federal or state government agencies. In some cases, the law may require the sharing (such as in a response to a request from Congress, or for a security incident involving information contained in the CRS). In other cases, sharing the information may be necessary to help respond to your contact, share complaint data relevant to another agency’s regulatory authority, or for law-enforcement. The CFPB has fully documented the ways in which it may share information from the CRS under its “Routine Uses” section of the SORN, CFPB.005 – Consumer Response System.

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

The CFPB collects the information contained in the CRS directly from individuals who have chosen to submit a contact about a consumer financial product, service or entity.

The CFPB may also collect a limited amount of information relevant to an individual's complaint from the entity that is the subject of the complaint. This may include information about the individual (including financial information) that the entity uses in resolving or responding to an individual's complaint.

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

The CRS interacts with other internal CFPB systems in order to inform other CFPB functions, such as supervision and enforcement. In most cases, the CRS receives some information back from those systems.

The CFPB has data sharing agreements and memoranda of understanding in place between itself and its partner agencies at the state and federal level for sharing data from the CRS. In cases where the CFPB directly transfers CRS data to or receives other data from another federal or state agency, the CFPB only shares that information through secure channels in processes that are governed by Interagency Security Agreements.

In some cases, the CFBP may share information via an extract from the CRS.

Entities that are the subject of consumer complaints made to the CFPB also access a subset of CRS data so that they can view and respond to complaints about them. This access includes daily downloads through a secure channel called the "Company Portal" that each entity must log into.

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 no risks associated with use limitation for this system.

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?

Individuals provide information to the CRS either through the form at ConsumerFinance.gov, through a physical form, or over the phone. If it is over the phone, our customer service representatives make sure

that they accurately record what the individual wants to submit. If individuals use the web or physical form, the CFPB assumes they entered the info correctly and does not verify the information for accuracy or completeness at the time of collection. If the CFPB follows up with a consumer and that consumer notices that something is wrong, they can amend, correct, or otherwise update their information. In addition, limited verification may occur if the CFPB directly communicates with a complaint subject or works with a representative of the entity that the contact regarded. For example, if you complain about a credit card rate from a credit card issuer, then the CFPB may work with that credit card issuer to research your complaint, including validating some of the information in your complaint.

If the CFPB later uses information collected through a contact for supervisory or enforcement purposes, each of those systems would validate the information.

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?

Individuals provide the information in the CRS by submitting a contact either through the form at ConsumerFinance.gov, through a physical form, or over the phone. If it is over the phone, our customer service representatives make sure that they accurately record what the individual wants to submit. If individuals use the web or physical form, the CFPB assumes they entered the info correctly and does not verify the information for accuracy or completeness at the time of collection. If the CFPB follows up with consumers and they notice that something is wrong, they can amend, correct, or otherwise update their information.

There is a risk that information contained in the system may be erroneous, incomplete, or outdated. However, depending on how individuals choose to submit a contact, built-in processes and controls exist to limit the chance of erroneous information being included. Customer service representatives guide individuals who choose to submit contacts via telephone on what information to provide. The customer service representative taking the complaint also confirms the information with the individual before submitting the contact. Individuals who choose to use the web form have an opportunity to review the information provided before submitting.

Individuals may later amend, correct, or otherwise update information in some types of contacts – such as a complaint – if that individual has chosen to create an account in order to access those contacts after submission. The CFPB does not validate the information at the time it is initially collected, but may validate at a very basic level in the course of referring or responding to a contact – especially if the CFPB refers a complaint to the entity that is the subject of the complaint. The CFPB may gather additional information if it works with the entity or the consumer to further investigate a contact. The CFPB may use this information to help validate information provided in the initial contact.

In addition to following up on a contact to update, amend or correct information where possible, the CFPB also provides individuals a means through the Privacy Act to amend or correct a person's records at their request or the request of their Congressional representative. Information about Privacy Act requests is available in the SORN, CFPB.005 – Consumer Response System, and at <http://www.consumerfinance.gov/foia>.

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 limits access to the CRS to employees and contractors with job functions related to responding to, referring, or otherwise investigating a contact. Additionally, the CFPB grants system access to contractors acting on behalf of the CFPB as customer service representatives. The CFPB also grants limited CRS access to approved users from entities that are the subject of complaints. Users from these entities access the CRS through a portal that allows them to view contacts related to that entity. Entities use this portal to facilitate providing a response to both the consumer and the CFPB regarding a contact. This portal is only accessible via a secure channel using a CFPB issued login and password. The CFPB may also provide this information directly to the entity.

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 – have their access removed appropriately.

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

The CRS was issued an Authority to Operate (“ATO”) at the Moderate level by CFPB. The ATO was signed on July 14, 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 CRS. The CFPB may also maintain information in locked file cabinets or rooms with access limited to those personnel whose official duties require access. Limited access for entities that are the subject of information in the CRS is available through a portal. 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 CRS.

The CFPB has implemented extensive security controls and safeguards for the CRS 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.

Additionally, the CFPB has worked closely with the CRS vendor to ensure that appropriate disaster mitigation strategies, breach notification processes and plans, and secure channels for submitting transactional information are in place for the system.

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

The CFPB and the contracted vendor have developed an incident-reporting plan and procedures for handling a security incident involving the CRS. The vendor's Security Operations Center monitors daily use of the system and is responsible for reporting any incidents directly to the CFPB's Information Systems Security Officer who coordinates all escalation, reporting and response procedures on behalf of the Bureau.

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 because the CRS will include large amounts of information on consumers and their financial transactions, it will be considered a rich target for hackers, identity thieves, and other cyber-threats. The CFPB has mitigated this risk by implementing extensive security controls and safeguards for the CRS to protect information contained in the system against unauthorized disclosure and access.

There is also a risk that unauthorized individuals may gain access to the information in the CRS. The CFPB has mitigated this risk by only granting access to the system to authorized users who, based on their need to know, are restricted to the minimal amount of data required or appropriate to carry out their assigned job responsibilities. Access is terminated or reduced as necessary should the employee or contractor no longer have a need to know the information, change job functions, is terminated or resigns.

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.

You must actively choose to submit a contact, and can limit how much of your personal information you provide when doing so. Moreover, you can make your contact anonymous. In some cases you have the ability to determine if you would like your personal information shared with the institution that is the subject of the contact (as is the case with those who self-identify as victims of discrimination or employees of the institution that is the subject of a complaint).

Individuals who are mentioned in contacts – such as employees of an institution to which the contact pertains – may not be notified that contacts mention them.

The CFPB's intake forms for contacts guides the individual to provide only that information which is relevant and necessary to provide follow-up; however, in providing information in a contact, individuals may provide some PII about other individuals at the entity that is the subject of the contact.

7.2 What procedures will allow individuals to access their information?

The CFPB provides a means through the Privacy Act of amending or correcting your records at your request. Information about Privacy Act requests is available in the SORN, CFPB.005 –Consumer Response System, and at <http://www.consumerfinance.gov/foia>.

You may also amend or update information contained in some types of contacts if you create an account when you submit a contact. The CFPB may also make additional corrections to information in the CRS if the CFPB gathers more information about your contact during a follow-up.

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

The CFPB provides a means through the Privacy Act of amending or correcting your information in the CRS, which is described above in Section 7.2.

You may also amend or update information contained in certain types of contacts (such as a complaint) if you create a user account when submitting the original contact. The CFPB may make additional corrections to information in the CRS after working with you to gather more information about your contact in a follow-up.

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 complaints could be filed on behalf of individuals without their consent. To mitigate this risk, the CFPB's complaint intake form requires individuals filing complaints on behalf of other individuals to prove that they are doing so with the knowledge and consent of the individuals they purport to represent.

A similar risk exists when individuals post contacts on behalf of others in the CFPB's online discussion forum or in its "Tell the CFPB" intake form. The CFPB does not take steps to mitigate this risk.

Finally, a risk exists that contacts could mention employees of financial institutions and personal information about such employees. . To help mitigate this risk, the CFPB's intake form for complaints and inquiries guides individuals to provide only that information which is relevant and necessary for the CFPB to follow-up.

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.

The CFPB provides specialized training for the consumer response team, and has requirements in place that require the contracting support to provide appropriate training in privacy and data security to customer service representatives.

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 provides its employees with appropriate privacy and security training to ensure information is used and secured appropriately. The CFPB has also implemented a rigorous set of security controls for the CRS, and has limited access to those CFPB employees with a clearly defined business need to know the information.

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 CFPB believes that its use of a contract service and private cloud environment for hosting and managing elements of its consumer complaint and inquiry functions provides the most cost-efficient, effective, and secure solution for delivering this critical element of its mission.

The CFPB has worked closely with the contracted vendor to implement policies and procedures, privacy and security training for users, and appropriate access controls and auditing capabilities for the CRS. The CFPB's Information Technology security personnel are able to access audit capabilities on an ad-hoc basis.

The CFPB and the vendor have developed an incident-reporting plan and procedures for handling a security incident involving the CRS.