

Industry, Expert, and Community Input, and Engagement

Does the CFPB use the information to benefit or make a determination about an individual?

No.

What is the purpose?

- Manage contact, relationship, and input information from external stakeholders.
- Conduct and publish research and other related information to improve understanding of consumer financial markets.

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, access, and redress.



Consumer Financial
Protection Bureau

A decorative graphic at the bottom of the page consisting of several overlapping, semi-transparent green shapes in various shades of green, creating a layered, abstract effect.

Overview

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

In pursuing its mission the CFPB will gather input on a variety of issues from interested stakeholders, including experts in consumer finance, representatives of industry, and members of the public (“Stakeholders”). The CFPB uses a variety of methods to engage and interact with Stakeholders. These interactions could include: Stakeholders expressing an interest in receiving information about the CFPB; correspondence between the CFPB and Stakeholders; input provided as a result of a CFPB-sponsored or facilitated meeting, interview, or focus group; participation in or attendance at CFPB-affiliated events; or participation in a CFPB-sponsored or affiliated advisory board.

The Bureau collects Personally Identifiable Information (PII) in order to manage some of these interactions. Generally, such PII is limited to name and contact information (e.g., address, email, phone number); however, for some interactions, more sensitive PII may be necessary. For example, the Bureau may collect the Social Security numbers (“SSN”) of individuals who serve on a Bureau advisory board in order to conduct due diligence screenings. The Industry, Expert, and Community Input and Engagement Privacy Impact Assessment (IECIE PIA) will cover such collections.

Access to all information, including PII, collected under the IECIE PIA will be limited to those offices with the most direct relationship with any given Stakeholder and on a need-to-know basis.

All information covered by the IECIE PIA is authorized by law. This information must be collected in accordance with and be compliant with other applicable federal laws, including other provisions of the Dodd-Frank Act, the Paperwork Reduction Act, the Right to Financial Privacy Act, and the Privacy Act of 1974.

There is no single system supporting the IECIE collection. Information is maintained within the CFPB’s authorized computing environments, including but not limited to the General Support System (“GSS”) with a number of Linux and Microsoft OS environments that host flat files or

SQL databases. Information may also be contained in authorized contractor environments, where all system details are documented and reported to CFPB on a recurring basis.

Where records are retrieved by personal identifier, the information may be documented in one or more System of Records Notices (SORN), including: CFPB.013, External Contact Database, 77 FR 59386; CFPB.016, CFPB Advisory Boards and Committees, 78 FR 25428; CFPB.017, Small Business Review Panels and Cost of Credit Consultations 77 FR 24183; and CFPB.021, Consumer Education and Engagement Records, 77 FR 60382.

In some cases, the IECIE PIA may implicate requirements in the Paperwork Reduction Act (“PRA”). In such cases, the Bureau complies with all PRA requirements.

In some scenarios, the CFPB may retain a third party to collect or work with information covered by the IECIE PIA. In such cases, the CFPB may use contracts, data sharing agreements, or other similar agreements or processes to ensure that the third party meets all applicable privacy and security requirements.

The CFPB may publish some information covered by the IECIE PIA in research reports, press releases, or through its website or third-party hosted social media, subject to applicable law, including the Bureau’s confidentiality regulations, 12 C.F.R. Part 1070 and approval process. These reports will be available to the public, and will not include any information that directly identifies an individual without that individual’s informed consent. The Bureau may also release non-direct identifying PII, but such releases would be limited to information that is otherwise publicly available.

Privacy Risk Analysis

The primary privacy risks associated with data covered by the IECIE PIA are risks related to:

- Confidentiality, and
- Data minimization and Data quality.

Confidentiality: In the event of a breach of confidentiality, there is a risk of embarrassment or loss of reputation to both the individual and the Bureau. Most of the information is low sensitivity and in the case of a breach the harm would be minimal. However, in cases where more sensitive PII is collected, a breach of confidentiality could result in consumers suffering financial harm or identity theft. The Bureau minimizes this risk by enforcing access controls to

minimize the number of individuals who have access to the data and by storing data on systems that have been accredited as secure for this type of data. Staff are also trained on how to handle potential breaches to minimize negative impacts.

Data Minimization and Data Quality: Through interactions with Stakeholders, the Bureau could on occasion obtain unnecessary or incorrect information. Because the interactions that result in information collection are generally voluntary, and because the Bureau does not use any information collected through these types of interactions to deprive an individual of a right or benefit, the privacy risks associated with these collections are minimal. Typically, Stakeholders choose what and how much information they share with the Bureau and they have opportunities to change or update information that is erroneous or no longer accurate or relevant. Direct identifying PII is generally limited to names and contact information (address, phone, email, professional affiliation or employer) necessary for facilitating communications or managing relationships. In limited situations, the Bureau may obtain PII from third-party sources – including state and federal agencies. In such cases, information is typically limited to that which is otherwise publicly available through web or public record searches and is generally about public figures in their professional capacity. In cases where information is obtained from non-public sources, the Bureau collects such information in accordance with applicable law and pursuant to applicable agreements governing the sharing of such information (e.g. Memoranda of Understanding, Memoranda of Agreement.) Finally, to minimize any residual impact on individuals, the CFPB has implemented appropriate technical, physical, and administrative controls relative to the risks presented to confidentiality, information quality, and information uses. These controls are discussed in more detail in the subsequent sections of this PIA.

Privacy Risk Management

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

Information collected for Industry, Expert, and Community Input and Engagement is typically collected directly from individuals, at their discretion and with consent, in order to facilitate communications between them and the Bureau. Impacted individuals vary based on the nature of the engagement, but generally include:

- Members of the public submitting formal public comments on Bureau-published notices or rulemakings;
- Practitioners and other service providers in the area of financial education and capability;
- Representatives of community organizations, employers, social workers, teachers, community organization leaders, etc., who interact with consumers;
- Representatives of industry, including representatives of covered persons as defined by the Bureau and employees of those entities;
- State and Federal government representatives, including members of the United States Congress and their staff;
- Individuals who apply to serve on a CFPB sponsored or affiliated advisory boards or councils;
- CFPB employees; and
- Other individuals, including consumers, who interact with, submit feedback to, or otherwise share information with the CFPB at their own discretion.

PII collected for general interactions may include:

- Name
- Address
- Phone Number (home or work)
- E-mail Address
- Employer/Professional Affiliation, including title
- Input and feedback from the public including comments, videos, links, and images.

More sensitive PII, collected only with informed consent, and only as necessary and for limited purposes such as access to CFPB information resources or facilities, or as part of a due diligence screening of individuals serving on CFPB advisory boards, etc., may include:

- Social Security number (*only if authorized by law*)
- Other information relevant to the CFPB's determination of an individual's eligibility for serving on a CFPB board or committee, including but not limited to:
 - Date and place of birth
 - Prior or pending civil or criminal actions against the individual;
 - Education
 - Registration in professional societies, membership on other boards and committees,
 - Professional or employment information, including resumes, CVs, work experience, and record of performance
 - Publications authored
 - Professional awards
 - Financial disclosure information
 - Declarations of desire and eligibility to serve
 - Lobbyist registrations
 - Names of professional references and notes and records of conversations with those references

In some cases, the Bureau may obtain information from publicly available sources or from other government sources such as other Federal and state agencies. Such information is generally limited to name, contact information, and other biographic information about individuals in their professional or public capacity. For example, the Bureau's External Affairs office may use the results of a Google search of publicly available data to compile biographical information about meeting participants prior to the meeting as part of a briefing book for Bureau leadership. In cases where the information is derived from non-public sources, such as other Federal agencies or data brokers, the Bureau obtains such information using contracts, information sharing agreements, or other similar agreements or processes, and in accordance with applicable law. Any directly-identifying PII released is done only with informed consent of the individual.

In some cases, the Bureau may release direct-identifying PII collected as part of a report or press release, or on its website or through a third-party website (i.e. social media). As an example, the Bureau's Consumer Education and Engagement office may conduct research into best practices in workplace financial education and, as a part of that research, may interview thought-leaders in the financial education community. The interviewed individuals may then, with their informed consent, be quoted in the study's resulting white paper.

Information collected for Industry, Expert, and Community Input and Engagement does not typically involve the use of forms or trigger the requirements of the PRA. However, in cases where the PRA requires it, the Bureau obtains approval of the Office of Management and Budget for such information collections.

2. Describe CFPB's objective for the information.

Information covered by this PIA is used to engage and interact with Stakeholders. Basic contact information is used for correspondence, to conduct interviews or focus groups, or to register participants or take attendance at a CFPB sponsored or facilitated event. The information may also be used to later identify individuals that are interested in specific issues in which the CFPB is engaging. In limited cases, the CFPB may collect more sensitive PII to facilitate engagement, specifically to conduct due diligence reviews on individuals who apply to serve on a CFPB sponsored or affiliated advisory body.

In some cases, the Bureau may release PII, with the informed consent of impacted individuals. Such releases are generally necessary for promoting transparency (CFPB events, membership on

CFPB advisory boards, responses to Congressional inquiries, etc.), or for raising awareness of CFPB and consumer finance issues through events or press releases, or may otherwise be required by law.

3. Describe how CFPB shares, for compatible purposes, any of the information with third parties, e.g. federal or state agencies, the general public.

In some cases, the CFPB may share information collected through Industry, Expert, Community Input and Engagement. In cases where this information includes PII, information will only be shared publicly with the consent of impacted individuals.

The nature of information sharing varies by the type of engagement. For example, individuals who attend a CFPB sponsored event may be recorded or photographed (and be informed of such recording) and have those images released as part of a press release or through the Bureau's social media channels. Likewise, individuals who are interviewed or serve on focus groups about consumer finance issues to inform a Bureau white paper or report are provided an opportunity to consent to have their participation acknowledged and be directly quoted. In other cases, such as membership on a Bureau-sponsored advisory board, the Bureau may release information about board members, with informed consent of participants, to the general public to promote transparency. Likewise, the Bureau may provide other state and Federal agencies or private third parties, information about applicants as part of a due diligence process (for example, providing the FBI an applicant's Social Security number as part of a due diligence screening.)

Where applicable, the CFPB may share information as outlined in the Routine Uses of the relevant SORN, CFPB.013, CFPB.016, CFPB.017, or CFPB.021.

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.

In general, individuals choose whether, and to what extent, they wish to share their information with the Bureau. Typically, individuals have opportunities to change or update information that is erroneous or no longer relevant. Notice may be provided through a Privacy Act Statement,

Privacy Notice, or, in some cases an alternative means, such as an Informed Consent form, via a third-party's privacy notice or policy, or through public notices (such as this PIA).

The CFPB provides a Privacy Act Statement, as required by the Privacy Act of 1974, when information is collected from respondents either by the CFPB or by contractors acting on behalf of the CFPB, and the information will be retrieved by personal identifier. The Privacy Act Statement is generally provided at the point where information is requested from individuals. Privacy Act Statements cite the applicable SORN; the authority under which the information is collected; whether disclosure of such information is mandatory or voluntary; the principal purpose or purposes for which the information is intended to be used; any routine uses which may be made of the information; and any effect of not providing all or any part of the requested information.

When the Privacy Act does not apply, the CFPB provides Stakeholders with a Privacy Notice. The Privacy Notice generally includes the same information as the Privacy Act Statement. However, the Privacy Notice does not cite a SORN as no SORN would be applicable. The Privacy Notice refers to the applicability of a third party privacy policy when appropriate.

The Bureau may also use other methods of providing notice – for example, an informed consent form, or directing individuals to the privacy policy of a third-party partner or vendor, or to the Bureau's own privacy policy for its website, consumerfinance.gov. Notice through a third-party website is provided in accordance with OMB Memorandum 10-23, "Guidance for Agency Use of Third-Party Websites and Applications."

The Bureau, or a third party acting on behalf of the Bureau, may provide Privacy Act Statements or Privacy Notices in different ways. For example, notice may be provided on the online registration form or sign-in sheet that is used to register Stakeholders for participation in a CFPB-sponsored event, the informed consent form used to acquire consent to release direct-identifying PII as part of a public report or news release, other types of information collection forms, or upon request. The notice is written in a language accessible to the Stakeholders and may be provided orally, telephonically, in hard copy, or online. In some cases, Stakeholders may be provided an opportunity to request a hard copy of the notice in addition to having it provided orally, telephonically, or online.

When a Privacy Act Statement is not required and when the provision of a complete Privacy Notice is not operationally feasible, a modified Privacy Notice may be provided. For example, in some cases, information may be retrieved from publicly available sources and notice is not

provided at the point of collection. In such cases, the Bureau has published this PIA and relies on a SORN (if applicable) and approval from the Office of Management and Budget of information collections under the PRA (if applicable) to provide notice to impacted individuals.

In the case of sharing information, the CFPB generally provides individuals with notice prior to their information being shared. In accordance with the Privacy Act, a Privacy Act Statement describes whether information may or may not be shared in accordance with the Routine Uses listed in the relevant SORN; and when the Privacy Act does not apply, a Privacy Notice is provided, which explains whether the information will be shared and, where applicable, how and with whom. Furthermore, in accordance with 5 CFR 1320.8(b)(3)(v), where applicable, CFPB information collections inform potential Respondents about the nature and extent of confidentiality to be provided, including the CFPB's rules on the disclosure of confidential information, including 12 CFR 1070.41(c), when they apply.

Where applicable, individuals may request access to or amendment of their information in accordance with the Privacy Act and the CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 *et seq.* Individuals may sometimes be able to directly update their information – for example, by contacting the Bureau directly to update contact or mailing information, or updating information provided for registration purposes for a Bureau-sponsored event.

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.

The CFPB complies with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002; adopts Office of Management and Budget privacy-related guidance as best practice;¹ and applies National Institute of Standards and Technology risk management processes for privacy.

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, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

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

- Audit Logs and Reviews
- CFPB Personnel Privacy Training, including annual and role-based training
- CFPB Privacy Incident Response and Recovery Plan and contractual obligations for third parties to support CFPB Privacy Incident Response and Recovery Plan
- Compliance with CFPB cybersecurity policy and procedures
- Information Quality and Integrity Checks
- Policy and Standard Operating Procedures, such as *Policy on Information Governance at the CFPB*, June 3, 2014
- Role-based Access Controls
- 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 (NARA): The CFPB will manage computer and paper records as permanent records until NARA approves the CFPB's records disposition schedule, at which time, the CFPB will dispose of such files in accordance with the schedule.. Records that fall under a general records schedule will be disposed of according to the applicable schedule.
- Personnel Security supported through due diligence screening

The CFPB may use contractors to help support the collection, use, disclosure, or retention of information covered by the IECIE PIA, and those contractors are subject to similar controls. Contractor access to information must occur in accordance with the Bureau's Policy on Information Governance.

Contractors with access to direct identifying PII are required to report suspected or confirmed privacy incidents to the CFPB immediately and no later than one hour after discovery. Other requirements placed on contractors may include: training on privacy, and compliance with federal privacy requirements and Federal Acquisition Regulations.

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.)

The CFPB may partner with other Federal, state, or local government agencies in the collection and use of information in support of activities associated with the IECIE PIA. In these instances, controls are put in place to protect against inappropriate collection, use, disclosure, and retention. The specific controls will vary based on the specific sharing. Typical controls would include:

- Compliance with CFPB cybersecurity policy and procedures,
- Data Quality and Integrity Checks,
- Extract logging and 90-day reviews,
- Policy and Standard Operating Procedures, and
- Role-based Access Controls.

Document control

Approval

Ashwin Vasan

Chief Information Officer

Date

Claire Stapleton

Chief Privacy Officer

Date

Name

Initiative Owner

Date

Change control

| Version | Summary of material changes | Pages affected | Date of change |
|---------|-----------------------------|----------------|----------------|
| | | | |
| | | | |