Nonbank Registry System

Privacy Impact Assessment

September 2024

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the Act)[1] established the Consumer Financial Protection Bureau (CFPB or Bureau). The CFPB is a 21st century agency that implements and enforces Federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive. The Act requires the CFPB to monitor markets for consumer financial products and services for risks to consumers to support its various functions and authorizes the CFPB to establish a nonbank registration program.

Pursuant to sections 1022(b) and (c) and 1024(b) of the Act, the CFPB issued the Registry of Nonbank Covered Persons Subject to Certain Agency and Court Orders Final Rule—referred to as the Orders Rule—on June 3, 2024.[2] The Orders Rule generally requires nonbank covered persons (hereinafter referred to as "nonbanks"), including nonbanks subject to the CFPB's supervisory authority, to register with the CFPB if they meet certain criteria as discussed below. Generally, "nonbanks" are companies involved in the offering or provision of consumer financial products or services that are not insured depository institutions or insured credit unions. To facilitate the nonbank registration program, the CFPB Supervision Division (Supervision) developed the Nonbank Registry (NBR) System—also known as the Nonbank Registry or registry—and external-facing portal—known as the Nonbank Registry Portal—to collect, use, and maintain information on nonbanks.

Through the Nonbank Registry Portal, nonbanks are required to register certain final public orders, including consent and stipulated orders and judgments (hereinafter referred to as "covered orders")[3] obtained or issued by the CFPB or any other government agency (federal, state, tribal, or local) based on the violation of certain consumer financial laws. Public agency or court orders are legally binding orders intended to prevent and remedy violations of the covered law. When an agency issues such an order, or seeks a court order, it typically has determined that the problems at the applicable nonbank are sufficiently serious to merit the expenditure of that agency's limited resources and perhaps the attention of the courts. The Orders Rule only pertains to covered orders that are "public," *i.e.*, that previously have been published by the issuing agency and/or court (or were required to be published by the issuing agency or court). To prevent the unnecessary disclosure of information maintained in covered orders, covered nonbanks are instructed in the

[1] Public Law No. 111-203, Title X.

[2] REGISTRY OF NONBANK COVERED PERSONS SUBJECT TO CERTAIN AGENCY AND COURT ORDERS 89 Fed. Reg. 56028 (June 3, 2024) *available at* https://www.federalregister.gov/public-inspection/2024-12689/registry-of-nonbank-covered-persons-subject-to-certain-agency-and-court-orders.

[3] *See* § 1092.201(e).

Orders Rule to redact any nonpublic portions of the covered orders before submitting them to the registry.

Additionally, the Orders Rule requires certain registered nonbanks subject to the CFPB's supervisory authority to submit on an annual basis a written statement signed by a senior executive (hereinafter referred to as "attesting executive" or "executive") with respect to the nonbank's compliance with the covered order during the preceding calendar year. The statement will generally describe the steps undertaken by the executive to review and oversee the nonbank's activities subject to the applicable covered order for the preceding calendar year. The executive will also provide a written, signed attestation regarding the nonbank's compliance with the covered order. The collection of this information allows the CFPB to prioritize supervision resources, assists in supervisory and examination activities (*e.g.*, potentially increasing supervisory effort related to some repeat offenders), improves accountability, and deters misconduct among nonbanks.

Finally, the Orders Rule allows the CFPB to publish some of the information collected from nonbanks for use by members of the public as well as other regulatory agencies. As stated in the Orders Rule, Congress authorized the CFPB to share its insights gained as the result of its market monitoring duties with a wider audience and granted the CFPB the authority to make non-confidential information available to the public "as is in the public interest."[4] However, publication is not mandatory. Therefore, the CFPB has sole discretion in determining whether to publish certain information maintained in the NBR System and the format of publication designed to protect confidential information in accordance with the Orders Rule.[5]

Nonbank Registry System

The NBR System resides within the CFPB Salesforce environment and leverages the capabilities of cloud architecture.[6] The CFPB established the NBR System to maintain information collected from nonbanks, including personally identifiable information (PII)[7] collected as part of

[4] 12 U.S.C. 5512(c)(3)(B).

[5] *Id.*

[6] *See* CONSUMER FINANCIAL PROTECTION BUREAU, PRIVACY IMPACT ASSESSMENT FOR THE SALESFORCE AND PLATFORM–CLOUD ENVIRONMENT (April 2022), and subsequent updates, *available at* https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[7] The term "personally identifiable information" is defined as information that can be used to distinguish or trace an individual's identity (*e.g.*, name, social security number, biometric records) either alone or when combined with other personal or identifying information which is linked or linkable to a specific individual (*e.g.*, date and place of birth, mother's maiden name).

the registration and document management process. In accordance with the Orders Rule, the CFPB is authorized to collect: (1) the nonbank's legal name (including any "doing business as [DBA]," or fictitious business names) and principal place of business address of the nonbank, state (or other jurisdiction) of incorporation or organization, and all applicable unique identifiers issued by a government agency or standards organization (*e.g.*, Nationwide Multistate Licensing System [NMLS] number); (2) the full name of the nonbank's authorized representative(s) submitting the information on behalf of the nonbank, including the representative's title, email address, and username and password (for account access); (3) the full name and title of an attesting executive (or executives); (4) copies of all non-exempt covered orders as described above, which may include the names of individuals (*e.g.*, consumer, consenting party, defendant) listed or included in a covered order and related public records, such as court or agency documents, or other documents provided to the registry; and (5) the names of any affiliates that are required to register with respect to the covered order.

In addition, the NBR System provides a helpdesk feature that allows members of the public to ask questions about the Orders Rule and for NBR account users (*i.e.*, nonbank authorized representative) to submit a question to the CFPB to help resolve a technical issue or issue related to the submission of information. The information submitted also includes PII such as the full name of the individual submitting the question and an email address that the CFPB uses to reply to questions or provide assistance as appropriate. The majority of records maintained within the NBR System is covered under the CFPB.030—Nonbank Registry SORN.[8]

Finally, the NBR System maintains PII collected from CFPB Staff[9] assigned to maintain the NBR System, which includes full names and email address, along with usernames and passwords. Access account records for CFPB Staff and external authorized system users (*i.e.*, nonbank representatives) are covered under the CFPB.014 Direct Registration and User Management System (DRUMS) SORN.[10]

The CFPB is publishing this new Privacy Impact Assessment (PIA) to document the privacy protections that are in place for the PII collected, used, shared, and maintained in the NBR System.

---

[8] *See* CFPB.030 – NONBANK REGISTRY SYSTEM OF RECORDS NOTICE, 89 Fed. Reg. 59900 (July 24, 2024) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/. (hereinafter NBR SORN).

[9] CFPB Staff is defined as all employees, interns, volunteers, consultants, contractors, and detailees assigned to CFPB.

[10] *See* CFPB.014—CFPB DIRECT REGISTRATION AND USER MANAGEMENT SYSTEM, 83 Fed. 23435 (June 21, 2018) and subsequent updates, *available at,* https://www.consumerfinance.gov/privacy/system-records-notices/.

Privacy Analysis and Risk Management

The CFPB conducts Privacy Impact Assessments (PIAs) on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002[11] and in alignment with Office of Management and Budget[12] (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with the NBR System that supports the CFPB's nonbank registration program pursuant to the Fair Information Practice Principles (FIPPs). This includes the design and implementation of administrative, technical, or physical safeguards or controls, as applicable.

1. Characterization of Information

1.1 Identify the information the CFPB collects, uses, disseminates, or maintains, and the individuals about whom the information pertains.

The NBR System collects information on authorized representatives, attesting executives, and in documents uploaded to the system (*i.e.*, the covered order, related public records, or other documents), individuals listed or included in the covered order, such as a consumer or respondent. The NBR System maintains all or some of the following PII about the authorized representative(s) associated with and authorized by the nonbank to manage the registration process under the Orders Rule for covered orders:

- Full name;
- Title;
- Email address; and
- Username and password.

The NBR System maintains the following PII about the executive(s) associated with and authorized by the nonbank to submit written annual statements under the Orders Rule for covered orders:

---

[11] 44 U.S.C. § 3501 note.

[12] Although pursuant to section 1017(a)(4)(E) of the Dodd Frank Wall Street Reform and Consumer Financial Protection Act, Public Law 111-203, the CFPB is not required to comply with OMB-issued guidance, it voluntarily follows OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

- Full name; and
- Title.

Documents uploaded to the NBR System may include the following PII on individuals (*e.g.*, consumer, consenting party, defendant) identified or listed in documents provided to the registry (*e.g.*, covered orders):

- Full name;[13]
- Title;
- Work address;
- Email address; and
- Telephone number.
- Any other information pertaining to the covered order (*e.g.*, violation of consumer financial law) that may be associated with the individual.

The NBR System also maintains the following PII on members of the public that submit a question related to the Orders Rule through the helpdesk feature or, through the registry, and on NBR account users requesting technical assistance:

- Full name; and
- Email address.

Finally, the NBR System maintains the following PII on CFPB Staff authorized to access and manage the NBR System:

- Full name;
- Email address;
- Username and password; and
- Access/Audit records.

[13] Documents provided to the registry could include other PII as well, depending on the content of the document and applicable court and agency practices and rules. For example, a covered order could include additional PII regarding respondent's counsel, officers, or other representatives, individual respondents, or a point of contact designated in a notice provision.

1.2 What are the sources of information and how is the information collected?

The CFPB collects information directly from the nonbank's authorized representative. The CFPB's Salesforce environment provides an external-facing and secure portal to the NBR System referred to as the Nonbank Registry Portal for the nonbank where an authorized representative can register the nonbank with the CFPB. To register the nonbank, the representative must complete the Company Point of Contact Information section on the registration form and the system will create a user account for the representative. During the account creation and registration process, the representative will enter the company's legal name and the address of the nonbank's principal place of business, along with other information such as an employer identification number (EIN) (if applicable). The representative must also provide their first and last name and business email address for the system to create the user account. After registering the nonbank, the system will require the representative to create a password and proceed through multi-factor authentication process for identity management purposes.

Once a nonbank representative's user account is created within the NBR System, the representative may add additional nonbank users (and similar PII for those users as collected from the representative), submit a "notification of non-registration," and/or complete the required information to register a covered order, via various secure web forms and, thereupon, may enter the following information:

- Identify whether the nonbank is a covered nonbank as defined in the Orders Rule.
- For supervised registered entities, the name and title of the attesting executive who is responsible for and knowledgeable of the supervised registered entity's efforts to comply with the covered order (one attesting executive for each covered order).
- The agency(ies) and/or court(s) that issued or obtained the covered order, as applicable.
- The names of any affiliates that are required to register with respect to the covered order.
- Any order number, case number, docket number, or other identifying number(s) of the covered order assigned by the agency or court.
- The effective date of the covered order and expiration date.
- Information regarding the covered law(s) alleged to have been violated.

The representative also uploads a copy of the covered order(s), which—as noted above—may contain the full names and certain other PII, such as title, work address, phone number, and email address (as noted above) of individuals listed or included therein.

For nonbanks that are not a covered nonbank or supervised registered entity (or believe that any orders issued against them do not qualify as "covered orders"), the information collection may be limited to the registration process. The nonbank representative can then submit a notification of non-registration in the "Notices to CFPB" section on the Company Profile tab, by either uploading a PDF or textbox entry containing information regarding the nonbank's good-faith belief that the nonbank is not a covered nonbank, that the order in question is not a covered order, and/or that the organization is not a supervised registered entity, or that a previously submitted notification of nonregistration is no longer applicable.

Finally, the NBR System collects information directly from CFPB Staff that maintain it, and members of the public that may submit a question about the Orders Rule through the NBR helpdesk feature. The NBR System provides a secure web form where representatives provide their full name and email address, along with a question or description of the issue that requires resolution by the CFPB.

1.3 If the information collection is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number for the collection.

The information collection contained in the "Registry of Nonbank Covered Persons Subject to Certain Agency and Court Orders" Rule was submitted to the Office of Management and Budget (OMB) for approval at the Notice of Proposed Rulemaking stage and the Final Rule stage and has been assigned the OMB control number 3170-0076.[14]

1.4 Discuss how the accuracy of the information is ensured.

The information maintained in the NBR System is collected directly from the nonbank's authorized representative or other approved users and, as applicable, attesting executive(s). The nonbank is responsible for providing accurate information at the time of collection. Additionally, pursuant to the Orders Rule, the nonbank is required to update its information maintained in the NBR System.

For example, if a nonbank changes its legal name or relocates its principal place of business, the nonbank is required to notify the CFPB. If the nonbank wishes to update or correct its

[14] *See* CONSUMER FINANICAL PROTECTION BUREAU, REGISTRY OF NONBANK COVERED PERSONS SUBJECT TO CERTAIN AGENCY AND COURT ORDERS, OMB Control No. 3170-0076, *available at*, https://www.federalregister.gov/documents/2024/07/08/2024-12689/registry-of-nonbank-covered-persons-subject-to-certain-agency-and-court-orders.

information within in the NBR System, the nonbank's authorized representative can log into their user account via the Nonbank Registry Portal and directly access and/or amend the information (*e.g.*, email address, principal place of business) maintained in the NBR System.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that information collected and maintained in the NBR System may be inaccurate.

Mitigation: To mitigate this risk, the CFPB collects the information maintained in the system directly from the individuals who are representatives of the nonbank, thereby increasing the likelihood that the information in the NBR System is accurate. As noted above, the Orders Rule requires the nonbank to provide accurate information at the time of collection and periodically update its information maintained within the NBR System to ensure its accuracy and completeness.[15] If the nonbank is unable to update its information due to a technical issue, it may contact the CFPB using the helpdesk feature and CFPB Staff will work with nonbank to resolve the issue. Additionally, the NBR System includes a disclaimer available via a link at the bottom of every page, which provides a link to the filing guidelines and the CFPB's website for details for details about the Orders Rule. The disclaimer reminds the nonbank that information provided via the Nonbank Registry Portal must be updated and states the following:

> *This is where you will register your company's covered order. If your company has more than one covered order, each covered order will require its own registration. Visit the CFPB's public website for more information, including what is a covered order.*
>
> *You are required to submit revised and final filings of already-registered orders. For an order that is modified and remains in effect, you are required to revise the information below within ninety (90) days of the effective date of such modification. For an order that is fully terminated or abrogated in relevant part and no longer remains in effect, or is no longer a covered order, you are required to submit a final filing. Click here for more information, including instructions on how to submit a revised filing or a final filing.*

[15] Orders Rule, *supra* note 2.

You will need the final public covered order (Order) to complete this registration.
To upload the Order, it must be in PDF format and less than one (1).

Finally, CFPB Staff may routinely review documents submitted through the portal. Any documents identified as inadvertently uploaded to the NBR System or not relevant to the Orders Rule may be removed by CFPB Staff to prevent the unnecessary collection of PII or other sensitive information within the NBR System. For information shared with other CFPB programs, it is the responsibility of the receiving program office to verify the accuracy of information maintained in the NBR System based on the program's mission purpose and use.

2. Limits on Information Collection and Retention

2.1 Explain how the CFPB only collects and maintains the information that is directly relevant and necessary to accomplish the specified purpose(s).

The CFPB only collects a limited amount of information about individuals that is narrowly tailored to effectively facilitate the nonbank registration program. Nonbanks are required to register with the CFPB upon becoming subject to a public written order imposing obligations based on alleged violations of certain consumer-protection laws. These nonbanks are required to register in the NBR System and provide basic identifying information about the nonbank and the covered order, including a copy of the covered order.

As noted above, the covered order may contain the names and other PII (*e.g.*, contact information) of individuals identified or listed therein. A copy of the covered order is relevant and necessary as it helps the CFPB more clearly identify the covered orders to which the registered entity is subject, as well as the terms of those orders, and provides access to updated copies of those orders.

The nonbank must also identify an authorized representative that will facilitate the registration and document management process on behalf of the nonbank. The PII collected and maintained on the nonbank's authorized representative is limited to their name and email address. This information is necessary and used to create a nonbank user account within the NBR System. User accounts are required for registration with the CFPB through the Nonbank Registry Portal.

Additionally, for certain nonbanks subject to the CFPB's supervisory authority, the CFPB will collect and maintain the name and title of an executive (or executives) identified by the nonbank. This is information that allows the CFPB to identify executives responsible for and knowledgeable of the nonbank's efforts to comply with covered orders. The supervised nonbank will also be required to submit, on an annual basis, a written statement signed by the applicable executive

regarding the nonbank's compliance with each applicable covered order. The written statement will also describe the steps the executive has undertaken to review and oversee the nonbank's activities subject to the applicable covered order for the preceding calendar year. The submission of an annual written statement will facilitate the CFPB's supervision and assessment and detection of risks to consumers and allow the CFPB to consider supervised nonbanks' compliance record regarding consumer-protection law when prioritizing supervisory resources.

Finally, the system collects PII on CFPB Staff. PII is limited to full name, title, and email address, and usernames and passwords. This information is required to create user accounts and access CFPB systems. The information is also used in audit logs that may be used to verify compliance with CFPB's privacy and security policies.

2.2 Describe the records retention requirements for the information. Has the retention schedule been approved by the CFPB and the National Archives and Records Administration (NARA)? If so, include the retention schedule.

The CFPB's Records and Information Management program collaborates with program managers to develop records retention schedules and submits to the National Archives and Records Administration (NARA) for appraisal. NARA provides the authority to disposition when records retention schedules are approved.

Currently, there is no NARA-approved records retention schedule for NBR records. Therefore, the records are unscheduled and considered permanent in nature until NARA's approval to disposition is obtained. The official records are managed within the NBR System. Standard operating procedures (SOP) and associated instructional documentation are managed within the NBR System, Supervision's records repository, and consumerfinance.gov.

Privacy Impact Analysis: Related to Limits on Information Collection and Retention

Privacy Risk: There is a risk that information maintained in the NBR System will be retained longer than necessary to accomplish the purpose for which it was originally collected.

Mitigation: While the records collected and maintained in the NBR System are unscheduled, the CFPB's Records and Information Management program in coordination with Supervision is currently in the process of drafting a Bureau records schedule for the NBR System to be approved

by NARA. The estimated time for completion and publication of the Nonbank Registry records schedule is by September 2025.[16]

Privacy Risk: There is a risk that the NBR System collects more information than is necessary for the purpose of the nonbank registration program.

Mitigation: To mitigate this risk, the CFPB has established technical controls and privacy safeguards to collect only a limited amount of information. First, as noted above, the collection of PII is limited to the name and email address for authorized representatives, which is required to create nonbank user accounts and facilitate the nonbank registration process. Similarly, the collection of PII for nonbank executives is limited to their name and title to identify those responsible for and knowledgeable of the nonbank's efforts to comply with covered orders submitted via the Nonbank Registry Portal as part of the nonbank registration program.

Second, the NBR System is designed to only collect the information required pursuant to the Orders Rule. For example, the Nonbank Registry Portal uses web forms to limit the collection of PII and other sensitive information (*e.g.*, proprietary information) required for the registration and document management processes. The portal and data fields include additional information to guide the nonbank through the registration process, and additional information is provided for certain points in the information collection to ensure the nonbank provides only the information required.

Additionally, the NBR System is designed to prohibit the collection of highly sensitive information and comply with the Orders Rule. As noted in the Orders Rule, a registered entity should not submit any Social Security numbers, individual taxpayer identification numbers, or other similar personally identifying tax information to the nonbank registry, even if the registered entity uses an individual's Social Security Number (SSN) in tax documents filed by or associated with the entity. The system will not allow for entry of a SSN where, for example, an SSN may also be used in lieu of another identification number as in the case of sole proprietors. To prevent the unnecessary collection of SSNs, the system automatically disables the data field that collects the identifier upon the user's selection of SSN as an option from the drop-down list rather than the Federal Tax Identification Number (TIN) or other available employer identifier. Therefore, even if the user attempts to provide the SSN as an employer identifier by selecting it from the drop-down list, they would not be able to enter it into the system to ensure compliance with the Orders Rule and limit the unnecessary collection of PII.

Finally, details on how to register will be provided through filing instructions available on the CFPB's NBR information landing page on the CFPB's external website. The NBR *Filing*

[16] https://www.archives.gov/research/guide-fed-records

Instructions Guide provides guidance on how to register and an easy-to-use summary of the requirements to assist with implementation of the Nonbank Registry Regulation. This guide is the definitive source of information for submitting information to the Nonbank Registry, as explained in the preamble of the NBR Orders Final Rule.

3. Uses of Information

3.1 Describe the purpose of the information and how the CFPB uses it.

The CFPB is responsible for regulating (among other things) the offering and provision of consumer financial products and services under federal consumer financial laws.[17] CFPB collects the information maintained in the NBR System to support its supervision, market monitoring, and other functions, and protects consumers from unfair, deceptive, and abusive practices when obtaining consumer financial products or services. More specifically, the CFPB uses this information:

- To effectively monitor and understand financial markets related to nonbanks.
- To monitor for and identify risks to consumers in the offering or provision of consumer financial products or services, including developments in markets for such products and services.
- To facilitate the CFPB's risk-based nonbank supervision program.
- To ensure that registered nonbanks subject to the CFPB's supervisory authority are legitimate entities and are able to perform their obligations to consumers, including their obligations under federal consumer financial law.

Additionally, information collected through the NBR System's helpdesk feature allows the CFPB to address questions submitted by members of the public regarding the Orders Rule and resolve technical issues for nonbank account users. Information collected on CFPB Staff (*e.g.*, names, usernames and passwords) is used to grant system access to those who support the NBR System and program operations and to maintain audit records. Finally, as discussed in more detail below, the CFPB may maintain a public registry hosted on the CFPB's website that may be accessed and used by members of the public and other regulators to facilitate public awareness and oversight.

[17] 12 U.S.C. 5511.

3.2 Is the information used or shared with other CFPB programs, systems, or projects?

Information maintained in the NBR System will be shared with users throughout Supervision, including examiners. Information may also be shared with other program offices to support CFPB mission operations in accordance with all laws, regulations, and policies. For example, the information may be shared with the Division of Research, Monitoring, and Regulations to help inform and prioritize the Bureau's market-monitoring efforts, including research regarding particular markets and the risk to consumers presented in such markets. Likewise, the CFPB's rulemaking efforts will benefit from the information about such covered orders, so that the Bureau might, for example, consider drafting rules to address identified consumer risks.

The CFPB's Office of Consumer Response will be informed by increased monitoring of risks and trends impacting consumer complaints through this information. The Office of Consumer Education may also receive this information to direct its effort to educating consumers about risks identified via the registry. Finally, the information may be valuable to the CFPB's Division of Enforcement to, among other things, inform whether a covered person is engaging, or has engaged, in conduct that poses risks to consumer regarding the offering or provision of consumer financial products or services.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that PII collected on nonbanks will be shared with individuals that do not have a need to know and used in a manner that is inconsistent with the original purpose(s) for collection.

Mitigation: To mitigate this risk, the CFPB only shares information maintained in the NBR System in accordance with laws, regulations, policies and CFPB SORNs. CFPB Staff that require elevated privileges to complete their job functions must sign and electronically submit the *Privileged User Access (PUA) Form* to obtain elevated access to the NBR System and review and acknowledge the *Rules of Behavior for Privileged Users*. The rules of behavior define the user's responsibilities, such as confirming that they will protect information from misuse and ensure information is only disclosed to authorized individuals that have a need to know.

All CFPB Staff are required to only share information when permitted by the CFPB's rules governing the Disclosure of Records and Information.[18] For example, confidential CFPB

[18] *See* 12 CFR Part 1070.

information may only be shared with CFPB employees, contractors, or consultants when such disclosure is relevant to the performance of their assigned duties.

Additionally, all CFPB Staff with access to CFPB systems, such as the NBR System, must sign the CFPB "Acceptable Use of CFPB Information Technology Resources" policy.[19] This policy establishes the user's responsibilities and the requirements to safeguard information technology resources and information. This includes protecting PII and other sensitive or confidential information. Finally, all CFPB Staff are required to comply with privacy policy and complete privacy training when they initially onboard and on an annual basis thereafter. CFPB privacy training stresses the importance of appropriate and authorized use of personal information in government information systems.

4. Individual Notice and Participation

4.1 Describe what opportunities, if any, individuals to whom the information pertains receive notice prior to the collection of information. If notice is not provided, explain why not.

General notice is provided by the CFPB through the publication of its rulemakings, this PIA, and the CFPB.030—Nonbank Registry SORN.[20] In addition, for NBR account users, the Nonbank Registry Portal provides a link to NBR's Privacy Act Statement prior to the information collection. A link to the Privacy Act Statement is also provided to members of the public that submit a question about the Orders Rule or NBR users requiring technical assistance on the CFPB's NBR information landing page on the CFPB's external website. The NBR Privacy Act Statement identifies the CFPB's authority under which the information is collected, the principal purpose(s) for which the information is intended to be used, and how the information may be disclosed, including the applicable SORN that applies. The Privacy Act Statement also informs the individual of the consequences for failing to provide their information.

[19] *See* ACCEPTABLE USE OF CFPB INFORMATION TECHNOLOGY RESOURCES, Operational Policy No. OPS-T&I-2023-07, Ver. 3.0 (April 9, 2023) and subsequent updates (hereinafter AUP).

[20] NBR SORN, *supra* note 8.

4.2 Describe what opportunities are available for individuals to consent to use, decline to provide information, or opt out of the CFPB's collection and use of the information.

Nonbank representatives and executives authorized to act on behalf of the nonbank cannot opt out or decline to provide their information. Pursuant to the Orders Rule, the nonbank's representative must provide their name and email address for nonbank registration and document-management purposes. Similarly, certain nonbanks subject to the CFPB's supervisory authority under 12 U.S.C. 5514(a) are required to annually identify an executive(s) responsible for and knowledgeable of the nonbank's efforts to comply with the covered orders identified in the NBR System. Additionally, such nonbanks will be required to submit on an annual basis a written statement signed by the applicable executive regarding the nonbank's compliance with each covered order. Finally, individuals identified or listed in covered orders and other public documents do not have an opportunity to opt out of the submission of such orders to the NBR System.

4.3 What are the procedures that allow individuals to access their information or correct inaccurate information?

Nonbank representatives have account access to the NBR System via the Nonbank Registry Portal and are required to maintain and update the information submitted to the system. For example, if a nonbank changes its legal name or relocates its principal place of business, the nonbank is required to have a representative update its information in the NBR System via the portal. The CFPB has established access and correction procedures for individuals that do not have account access, such as members of the public that submit a question about the Orders Rule.

Regardless of citizenship, individuals may access or correct their information maintained in the NBR System by contacting the CFPB's Freedom of Information Act (FOIA) Office[21] in writing in accordance with the Bureau's Disclosure of Records and Information Rules, Subpart E-Privacy Act,[22] promulgated at 12 C.F.R. 1070.50 et seq. If you have any questions, please contact the CFPB FOIA Office via FOIA@CFPB.gov or at (855) 444-3642.

[21] https://www.consumerfinance.gov/foia-requests/submit-request/

[22] eCFR 12 CFR Part 1070 - Disclosure of Records and Information

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that individuals identified or listed in covered orders do not have an opportunity to opt out or participate in the collection of their information maintained within the NBR System.

Mitigation: As noted above, covered orders submitted by the nonbank may contain the names and certain other PII of individuals identified or listed therein. Individuals identified or listed in covered orders or other public documents uploaded to the registry do not have the opportunity to opt out or participate in the collection of their information as these documents are required pursuant to the Orders Rule. The CFPB has taken steps to mitigate these risks by limiting covered orders to orders (or portions of orders) that are already public, thus limiting the sensitivity of the PII in the system.

5. External Sharing and Disclosure of Information

5.1 Does the CFPB share this information with external entities or partners? If so, identify the organization or third-party and how the information is accessed and used.

While the covered orders subject to the Orders Rule will already be public, information about the covered orders may not be readily accessible in a comprehensive and collected manner, and some of the information submitted to the NBR System may not be readily available to the public. As noted above, the CFPB may share certain information maintained in the NBR System with members of the public, including other regulators, through a public registry hosted on the CFPB's website, as well as through other means. The information maintained in the public registry may identify the nonbank and any attesting executive(s) associated with the nonbank (*i.e.*, name and title), if applicable, along with the covered order(s).

The purpose for sharing this information is to raise public awareness and to facilitate oversight. By improving public transparency, the CFPB intends to mitigate recidivism and more effectively deter unlawful behavior. For example, sharing this information with consumers and consumer advocacy groups would enhance the ability of these organizations to better understand and monitor the conduct of the entities with whom consumers do business. Publication will also facilitate the ability of consumers to identify the nonbanks that are registered with the CFPB.

Additionally, the publication of this information would create heightened accountability and have a deterrent effect on violations. For example, publication will enhance the ability of investors, research organizations, firms conducting due diligence, and the media to locate, review, and

monitor orders enforcing the law. Publishing such information in a public registry will, among other things, allow other regulators at the federal, tribal, state, and local level tasked with protecting consumers to realize many of the same market-monitoring benefits and assist the CFPB and others in developing new regulations and other reforms for consumer-protection.

Finally, the CFPB may share information in the NBR System directly with other federal, state, tribal, and local regulators to facilitate the work of those agencies, in accordance with its existing information-sharing agreements and protocols. For example, the Bureau may provide registry information to assist another agency in identifying a registered entity, or in identifying orders that may be in effect with respect to that entity. This will increase coordination between theses agencies and the CFPB and support supervision and law enforcement activities at all levels of government.

5.2 Does the CFPB place limitations on information sharing and/or re-dissemination of the information?

Yes. The CFPB may only share information with external parties via the public registry in accordance with the Orders Rule and the routine uses identified in the NBR SORN.[23] For example, the names of authorized representatives, along with their email address, will not be shared via the public registry. Additionally, the CFPB shares information with federal, state, tribal, and local regulators pursuant to the requirements set forth in the Act at 1022(c)(6)(A) & (C) and in the CFPB's regulations on Disclosure of Records and Information, and in accordance with information sharing agreements.

Privacy Impact Analysis: Related to External Sharing and Disclosure of Information

Privacy Risk: There is a risk that information may be shared in a manner that is inconsistent with the original collection.

Mitigation: To mitigate this risk, the CFPB has implemented administrative and technical access controls that help to ensure information maintained within the NBR System is used according to the purposes identified in this PIA and other related notices. Only CFPB Staff have direct access to all the information collected and maintained in the NBR System. As noted above, information is shared with external parties, such as other regulators based on a need to know and

[23] NBR SORN, *supra* note 8.

in accordance with the NBR SORN,[24] the CFPB's regulations on Disclosure of Records and Information, and information sharing agreements.

Finally, information disclosed in the public registry will be limited to nonbank identifying information, the name and title of the attesting executive (if applicable), and the covered order. To prevent the unnecessary disclosure of information maintained in covered orders, covered nonbanks are instructed in the Orders Rule to redact any nonpublic portions of the covered orders before submitting them to the registry. In order to avoid accidental publication of nonpublic information, the CFPB will conduct manual reviews prior to publication in order to mitigate any potential privacy risks, in accordance with applicable authorities.

Privacy Risk: There is a risk of unauthorized access or use by nonbank account users (i.e., authorized representatives).

Mitigation: To mitigate this risk, the CFPB has implemented security and privacy safeguards to protect CFPB systems and the information maintained within the NBR System. For example, the Nonbank Registry Portal resides within the CFPB network. As a federal database, the NBR system is subject to the Federal Information Security Modernization Act (FISMA),[25] which requires the annual verification that all users who access federal systems have both the business need and the authorization to access the system. To comply with FISMA, government users must annually verify employment and that their role requires continued access to the NBR System.

In addition, NBR account users are required to create user accounts via the Nonbank Registray Portal. NBR users can only log into their accounts with a username and password. NBR account users are also required to download and use a multi-factor authentication tool or application when logging into their user account. This tool will validate the NBR account user's identity every time they log into the NBR account. Additionally, nonbank entities are required to maintain at least one "Point of Contact" user that is responsible for assigning and managing information access within the NBR Portal for other users of the nonbank. The CFPB implements role-based access controls to ensure NBR users only have access to the system and/or information necessary and relevant to their assigned duties. This ensures that authorized nonbank representatives only have access to the system to allow them to upload documents to the NBR System and information pertaining to their organization.

Finally, the CFPB has established oversight controls to identify suspicious and/or authorized activity as discussed below in Section 6 of this PIA. For example, suspicious and/or unauthorized access is monitored and logged. Security administrators are notified of unusual behavior (e.g.,

---

[24] *Id.*

[25] Pub. Law No. 113-283.

disablement of security, login times, number of login attempts, failed login attempts) or misconduct (e.g., unauthorized removal of data) by authorized users.

6. Accountability, Auditing, and Security

6.1 How does the CFPB secure the information to ensure that it is used in accordance with stated practices in this PIA?

The CFPB complies with the Privacy Act of 1974,[26] the Right to Financial Privacy Act,[27] Section 208 of the E-Government Act of 2002, and other applicable laws. To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopts the Fair Information Practice Principles (FIPPs) as the framework for its privacy policy.[28] The FIPPs apply throughout the CFPB for the collection, use, maintenance, disclosure, and destruction of PII, and any other activity that impacts the privacy of individuals, regardless of citizenship, to ensure compliance with all laws, regulations, and policy requirements.

The CFPB adheres to the Office of Management and Budget (OMB) privacy-related guidance[29] and applies the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)[30] for information technology systems, applications, solutions, and services. The CFPB identifies and applies NIST SP-800-53[31] security and privacy controls and continuous monitoring of controls to ensure on-going compliance with information security standards and protect organizational operations and assets and individuals.

The NBR System has obtained an Authority to Operate from the CFPB's authorizing official.

---

[26] 5 U.S.C. § 552a.

[27] 12 U.S.C. §§ 3401-3423.

[28] *See* CFPB PRIVACY POLICY (Dec. 6, 2012), and subsequent updates.

[29] More information regarding OMB guidance is available at, https://www.whitehouse.gov/omb/information-regulatory-affairs/privacy/.

[30] *See* NIST, Risk Management Framework (RMF) For Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, SP-800-37 Revision (Rev.) 2 (December 2018). For more information visit https://www.nist.gov.

[31] *See* NIST, Security and Privacy Controls for Information Systems and Organizations, SP-800-53, Rev. 5 (September 2020). For more information visit https://www.nist.gov.

6.2 Describe what privacy training is provided to users either generally or specifically relevant to CFPB information system.

All CFPB Staff are required to adhere to all CFPB cybersecurity and privacy policies and take mandatory annual training. For example, CFPB Staff are required to take the CFPB Privacy Training and Security Awareness Training before being granted access to the NBR System and annually thereafter. The privacy training ensures that CFPC Staff understand their responsibilities to safeguard PII, and to identify and report suspected or confirmed privacy breaches within twenty-four hours of discovery. CFPB Privacy Office is notified of CFPB Staff that fail to complete the annual privacy training, at which time, their access is terminated until their annual privacy training is complete.

6.3 What procedures are in place to determine which users may access CFPB information systems and how the CFPB provides access?

CFPB Staff with access to CFPB information and systems and facilities are required to proceed through background investigations for suitability and security clearance determinations. This ensures compliance with all federal laws and that individuals supporting the CFPB are deemed reliable, trustworthy, and suitable for the role they will fulfill. Other requirements placed on federal contractors may also include those associated with Federal Acquisition Regulations.

CFPB Staff must properly obtain and present credentials to gain access to CFPB facilities and systems. The CFPB's secure access controls policy, "Secure Access Controls via Multi-Factor Authentication"[32] Policy applies to CFPB Staff that have logical and/or physical access to CFPB facilities, information systems or applications, and/or information (in physical or electronic form). This ensures the CFPB maintains a secure operating environment and protects our systems against potential external threats.

In addition, the CFPB employs role-based access controls. The CFPB uses role-based access controls to ensure CFPB Staff only have access to the system and/or information necessary and relevant to their assigned duties. System access is granted on the user's role within the NBR System. Individuals who no longer require access have their credentials removed from the system.

[32] *See* SECURE ACCESS CONTROLS VIA MULTI-FACTOR AUTHENTICATION, NO. OPS-ADMIN-2024-01 (Nov. 6, 2023), and subsequent updates.

Privacy Impact Analysis: Related to Accountability, Auditing, and Security

Privacy Risk: There is a risk that the NBR System and information maintained therein may be accessed by unauthorized individuals.

Mitigation: To mitigate this risk, the CFPB has implemented the above technical, physical, and administrative controls to safeguard PII and other sensitive information maintained in the NBR System. For example, access to the NBR System is limited to CFPB Staff who have a need to know the information in the performance of their duties. As noted above, CFPB Staff that require elevated privileges to complete their job functions must sign and electronically submit the *Privileged User Access (PUA) Form* to the CFPB ServiceDesk to obtain elevated access to NBR and review and acknowledge the *Rules of Behavior for Privileged Users*.

In addition, the CFPB has established oversight controls through robust auditing features to identify and support accountability for unauthorized use/misconduct. CFPB's "Information Governance" Policy[33] outlines the established rules on the intake, management, disclosure, and disposition of information (in its various formats) at CFPB and applies to all CFPB users. As noted above, CFPB Staff are required to review and sign the CFPB's "Acceptable Use of CFPB Technology Resources Policy"[34] and complete the privacy and security training, and annually thereafter, before access is granted to a CFPB system.

Suspicious and/or unauthorized access is monitored and logged, thereby discouraging users from inappropriate access to CFPB systems. Security administrators are notified of unusual behavior (e.g., disablement of security, login times, number of login attempts, failed login attempts) or misconduct (e.g., unauthorized removal of data) by authorized users. For example, the CFPB employs extract logging and 90-day reviews to identify user behavior and staff actions around particular events, such as changes in the information or data, warnings, or errors that are unexpected, which are reviewed in relation to their job roles and workflow. If the system administrator notices that anyone has used a system or application in violation of CFPB policy, system access may be revoked. If there is evidence of potential misconduct, the incident may be referred to the appropriate CFPB office for investigation and further review and appropriate action.

[33] *See* CFPB POLICY ON INFORMATION POLICY ON INFORMATION GOVERNANCE AT THE CFPB, No. OPS-OCDO-2023-18, 2.0 (Sept. 26, 2023), and subsequent updates.

[34] AUP, *supra* note 16.

Document Control

Approval

Chris Chilbert	**Kathryn Fong**
Chief Information Officer	**Chief Privacy Officer**
Katelyn Sellers	**Danny Pham**
Program/Product Owner	**System Owner**

Original, signed document on file with the CFPB Privacy Office

Change Control

Version	Summary of material changes	Pages affected	Date of change