Nationwide Mortgage Licensing System & Registry

Privacy Impact Assessment

February 2026

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act[1] (Dodd-Frank Act) 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.

In 2011, pursuant to the Dodd-Frank Act, the CFPB assumed: (1) supervisory and enforcement authority to ensure compliance with the Secure and Fair Enforcement for Mortgage Licensing Act of 2008[2] (SAFE Act), and (2) responsibility for developing and maintaining the SAFE Act federal registration system[3]. To implement the federal registration requirement of the SAFE Act, the CFPB established Regulation G, SAFE Mortgage Licensing Act-Federal Registration of Residential Mortgage Loan Originators[4].

The SAFE Act and its implementing Regulation G aim to protect consumers and reduce mortgage fraud by, among other things, requiring federal registration of residential mortgage loan originators (MLOs)[5] who work for a covered federal financial institution[6]. To obtain federal registration, MLOs use the Nationwide Multistate Licensing System and Registry (NMLSR), a centralized online database.[7] Thus, an individual is considered a federally registered MLO pursuant to the SAFE Act if that individual: (1) meets the definition of a MLO in Regulation G (12 C.F.R. 1007.102); (2) is an employee of a covered financial institution under Regulation G (12

---

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

[2] 12 U.S.C. §§ 5101 *et seq*.

[3] 12 U.S.C. § 5106.

[4] 12 C.F.R. Part 1007.

[5] In general, mortgage loan originator refers to an individual who: (i) takes a residential mortgage loan application; and (ii) offers or negotiates terms of a residential mortgage loan for compensation or gain. *See* 12 U.S.C. § 5102 (4) ('loan originator'); 12 C.F.R. § 1007.102 ('mortgage loan originator').

[6] Covered financial institution refers to any national bank, federal branch or agency of a foreign bank, member bank, insured state non-member bank (including state-licensed insured branches of foreign banks), savings association, or certain of their subsidiaries; branch or agency of a foreign bank or commercial lending company owned or controlled by a foreign bank; Farm Credit System institution; or federally insured credit union, including certain non-federally insured credit unions. *See* 12 C.F.R. 1007.101(c) and 102.

[7] 12 U.S.C. § 5102(6) (defining "Nationwide Mortgage Licensing System" as "a mortgage licensing system developed and maintained by the Conference of State Bank Supervisors and the American Association of Residential Mortgage Regulators for the State licensing and registration of State-licensed loan originators and the registration of registered loan originators or any system established by the Director [of the CFPB] under [12 U.S.C. 5108].)

C.F.R. 1007.102); (3) is registered pursuant to Regulation G with the NMLSR; and (4) CFPB assigns the individual an unique identifier[8] through the NMLSR. The SAFE Act and Regulation G require that the unique identifier not be used for any purpose other than those set forth in the SAFE Act.[9]

The CFPB has contracted with CSBS to maintain MLOs' federal registration information in the Registry, which is part of NMLSR. CSBS owns and manages the Nationwide Multistate Licensing System (NMLS)[10], while the CFPB owns the Registry (hereinafter Federal Registry), which is managed by its Supervision Division, Office of Supervision Policy & Operations (Supervision).[11] Therefore, this PIA focuses on the federal registration process within the Federal Registry, as well as the processes and procedures used to verify and maintain access to the NMLSR.

The Federal Registry electronically collects and maintains personally identifiable information (PII) and other information on MLOs seeking federal registration. Generally, this includes an individual's name, contact information, Social Security number, information about their current and past employment in the financial services industry, and information about any past civil or criminal actions taken against them.[12]

The Regulation G also requires MLOs to submit fingerprints and any appropriate identifying information to enable the Department of Justice, Federal Bureau of Investigation (FBI) to perform a criminal history background investigation.[13] This submission is also done through the NMLSR. The FBI conducts the criminal history records check and returns the criminal history records

---

[8] Unique identifier refers to a number or other identifier that: (1) permanently identifies a registered mortgage loan originator; (2) is assigned by protocols established by the Nationwide Mortgage Licensing System and Registry and the Bureau to facilitate: (i) electronic tracking of mortgage loan originators; and (ii) uniform identification of, and public access to, the employment history of and the publicly adjudicated disciplinary and enforcement actions against mortgage loan originators. See 12 U.S.C. § 5102 (13) ('unique identifier'); 12 C.F.R. 1007.102 ('unique identifier').

[9] *Id.*

[10] https://mortgage.nationwidelicensingsystem.org/knowledge/Products/nmls/aboutNMLS/SitePages/Home.aspx

[11] CSBS is the national organization responsible for the overall operation of NMLSR on behalf of state and federal regulators. For all other individuals, a state license and registration as a state-licensed MLO, along with a unique identifier, are required. NMLSR is operated by the State Regulatory Registry LLC (SRR), a wholly owned subsidiary of CSBS.

[12] 12 C.F.R. 1007.103.

[13] *Id.*

information (CHRI), which is then retained and stored within the NMLSR. The federal registration is activated and completed in the Federal Registry after the individual submits the filing, receives successful background investigation results, and the employer completes their review of the application.

In addition to MLOs information, the Federal Registry collects and maintains limited information about authorized individuals from covered financial institutions who are employees designated as primary contacts for federal agency regulated institutions or other individuals authorized to act on behalf of a covered federal financial institution to perform administrative tasks (herein collectively referred to as "authorized institution users"). Such tasks include submitting the MLO's identifying information for registration, maintaining federal institution records, administering the registration process for MLOs, and reviewing the MLOs' CHRI results. The Federal Registry also includes user information on CFPB Staff[14] and other federal agency employees who use the Federal Registry as part of their official duties to develop and maintain the system on behalf of CFPB (herein collectively referred to as "authorized federal users").

The FBI also requires that authorized institution users seeking access to MLO's CHRI be verified at the Identity Assurance Level 2 (IAL2) per NIST's Digital Identity Guidelines, NIST Special Publication (SP) 800-63A[15], before access to the Federal Registry is granted. This identity verification process is conducted on authorized institution users through a FedRAMP-authorized cloud service provider that is integrated with the NMLSR[16]. Once the identity of the authorized institution user is verified and permitted to access the Federal Registry, a "pass" marking is transmitted to the NMLSR, and access is granted to the individual. This is a one-time process unless the user changes their name in NMLSR, which would require the individual to reverify their identity through the FBI background investigation process.

Access to the minimum information required by the FBI to conduct a background check of an MLO is limited to the FBI for the purposes of conducting the required check, authorized NMLSR administrative users, and individuals representing financial institutions employed by the MLOs (typically the authorized institution user). Access to information required to conduct identity verification of authorized institution users is limited to the CSBS' third-party service provider (*i.e.*,

[14] CFPB Staff means all employees, interns, volunteers, contractors, and detailees assigned to CFPB.

[15] SP 800-63A-4, Digital Identity Guidelines: Identity Proofing and Enrollment | CSRC.

[16] The cloud service provider selected by CSBS to perform the identity verification has achieved Federal Risk and Authorization Management (FedRAMP) Authorization at FIPS 199 Moderate impact. A separate privacy assessment has been conducted by the vendor on the privacy controls implemented in their system.

contractor) and is not maintained by the FBI. Employees of the FBI are not authorized federal users of the system.

The SAFE Act and its implementing Regulation G also require that consumers be provided with easily accessible information about MLOs, at no cost and through electronic media.[17] This information includes, among others, the MLO name, the principal business location address and business contact information, the financial services-related employment history for 10 years prior to registration/renewal, and publicly adjudicated disciplinary and enforcement actions against MLOs. Additionally, the Federal Registry can be accessed by Federal banking agencies[18] and the Farm Credit Administration (FCA) (collectively referred to as the "federal agencies") responsible for regulating MLOs to access MLO information.

The Supervision Division retrieves records maintained within the Federal Registry using personal identifiers. These records are covered under the CFPB's System of Records Notice (SORN) titled CFPB.019 – Nationwide Mortgage Licensing System and Registry.

The original PIA for NMLSR was published in September 2012. The CFPB is updating the NMLSR PIA to clarify the CFPB's role and responsibilities for federal registration under the SAFE Act for NMLSR, to identify the information collection owned and managed by the CFPB for federally registered MLOs in the Federal Registry, to document the collection, use, maintenance, and dissemination of PII of MLOs and other system users maintained in the Federal Registry, and to describe the identity verification process that MLOs and authorized institution users undergo. This update also conforms with the CFPB's newest PIA template.

Privacy Analysis and Risk Management

The CFPB conducts PIAs on both programs and information technology systems, pursuant to Section 208[19] of the E-Government Act of 2002 and in alignment with Office of Management and Budget (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures for the Federal Registry portion of NMLSR pursuant to the Fair Information Practice Principles. This includes the design and implementation of administrative, technical, or physical safeguards or controls, as applicable.

---

[17] *See, e.g.*, 12 U.S.C. §§ 5101, 5106(b)(1); 12 C.F.R. 1007.103(d)(2)(iii). The NMLSR Consumer Access Portal is available at https://www.nmlsconsumeraccess.org/. See Appendix B of this PIA for more information about the NMLSR Consumer Access Portal.

[18] The "Federal banking agencies" include the Office of the Comptroller of the Currency , the Board of Governors of the Federal Reserve System , the Federal Deposit Insurance Corporation , and the National Credit Union Administration .

[19] 44 U.S.C. § 3501 note.

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 Federal Registry maintains information collected from MLOs (for initial registration or registration maintenance), authorized institution users, and authorized federal users.

The MLOs or the authorized institution users on behalf of the MLO provide the MLO federal registration information using the electronic Uniform Individual Mortgage Registration & Consent Form (MU4R). This information is collected and maintained in the Federal Registry and includes:[20]

- Full name (first, last, middle) and any other names used, if applicable;
- Home address and contact information (e.g., phone number, email);
- Principal business location address and business contact information;
- Social Security number (SSN)[21];
- Gender[22];
- Date and place of birth;
- Eye color and hair color;
- Race;
- Height;
- Weight;
- Financial services-related employment history for 10 years prior to the date of the MLO's registration or renewal;

[20] See 12 C.F.R. 1007.103(d), Required employee information.

[21] 12 C.F.R. 1007.103(d)(1)(i)(D).

[22] Under Executive Order 14168 of Jan. 20, 2025 (Defending Women From Gender Ideology Extremism and Restoring Biological Truth to the Federal Government), 12 C.F.R. 1007.103(d)(1)(i)(e) should refer to "sex" instead of "gender." The Bureau is continuing to work on implementing E.O. 14168 to reflect correct usage of the term "sex" instead of "gender.

- Current employment related information with the covered financial institution, including the date the employee became an employee of the covered financial institution;
- Convictions of any criminal offense involving dishonesty, breach of trust, or money laundering against the employee or organizations controlled by the employee, or agreements to enter into a pretrial diversion or similar program in connection with the prosecution for such offense(s);
- Civil judicial actions against the employee in connection with financial services-related activities, dismissals with settlements, or judicial findings that the employee violated financial services-related statutes or regulations, except for actions dismissed without a settlement agreement;
- Certain actions or orders by a state, Federal, or foreign financial regulatory authority;
- Revocation or suspension of the employee's authorization to act as an attorney, accountant, or state or Federal contractor;
- Customer-initiated financial services-related arbitration or civil action against the employee that required action, including settlements, or which resulted in a judgment; and,
- Fingerprints of the employee, in digital form if practicable, and any appropriate identifying information for submission to the FBI and any governmental agency or entity authorized to receive such information in connection with a state and national criminal history background check.

The CFPB also maintains the unique identifier assigned to the MLO through the NMLSR.

Additionally, authorized institution users and authorized federal users provide their information to establish a user account in the Federal Registry[23] using the electronic Uniform Mortgage Lender or Broker Application, Form (MU1R). This information includes:

- Full name;
- Contact information (email address, phone number); and
- Name of their institution or agency.

Finally, the following is collected from the authorized federal users to conduct the identity verification. This PII includes:

[23] 12 C.F.R. 1007.103(e)(1)(i)(E) and (F).

- Full name;
- Email address;
- Mobile phone number;
- Home address;
- Social Security number (SSN)[24];
- Date of birth;
- Photo of a government-issued ID (*e.g.*, passport, driver's license); and
- Photo of the individual.

Once the identity verification process is completed, CSBS, a CFPB contractor, retains the collected PII for continual verification, audit, and fraud review related to the registration and renewal process. The contractor retains PII, including name, email address, mobile phone number, home address, SSN, and date of birth, for re-verification purposes for 5 years, and a photo of government-issued ID and selfie photo for 3 years.

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

Information maintained within the Federal Registry is collected directly from the MLOs or the authorized institution user on behalf of the MLO for registration purposes, the authorized institution users for establishing accounts and identity verification, and the authorized federal users for establishing accounts using the forms described above. No information is collected from other systems to perform Federal Registry functions.

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

The information collected/gathered from the MU4R and MU1R forms by the CFPB and entered into NMLSR is authorized under the PRA as part of the information collection in Regulation G. The Bureau's OMB control number for this information collection is 3170-0005.

1.4 Discuss how the accuracy of the information is ensured.

The information maintained in the Federal Registry is collected directly from the MLO, authorized institution users, and/or authorized federal users. This increases the likelihood that the information provided is accurate and complete. These individuals are responsible for providing accurate information at the time of collection. Although authorized institution user may submit

[24] 12 C.F.R. 1007.103(d)(1)(i)(D).

registration information on behalf of MLOs, the MLO must attest to the correctness of the information submitted to the Registry during the initial registration process.[25]

Additionally, during the annual renewal registration process, only the MLO confirms and updates their information within the Federal Registry (*i.e.*, registration records). If the MLO fails to renew their registration, their registration will become inactive, and the individual cannot act as a federally registered MLO until the registration requirements are met.[26]

Finally, an MLO must update their registration within thirty (30) days for specified significant changes, including name changes, employment termination, and reportable changes to legal or regulatory actions. To update their information, MLOs may log into their NMLSR account within the Federal Registry and amend their information.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: There is a risk that information maintained in the Federal Registry is used for purposes beyond those described in this PIA.

Mitigation: To mitigate this risk, 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 Federal Registry 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 externally when permitted by the CFPB's rules governing the Disclosure of Records and Information.[27]

Additionally, all CFPB Staff with access to CFPB systems, such as the Federal Registry, must sign the CFPB "Acceptable Use of CFPB Information Technology Resources" policy. 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. Moreover, CFPB Staff are required to take annual privacy training. CFPB privacy training stresses the importance of the appropriate and authorized use of personal information in government information systems.

---

[25] 12 C.F.R. 1007.103(d)(2).

[26] 12 C.F.R. 1007.103(b).

[27] *See* 12 C.F.R. 1070, DISCLOSURE OF RECORDS AND INFORMATION, 78 Fed. Reg. 11483 (Mar. 18, 2013).

Finally, authorized federal users who are not CFPB Staff must submit a MU1R form for verification prior to gaining access to the system. These users are subject to identity verification and approval to use the system prior to gaining access.

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 information that is relevant and necessary using the MU4R (from MLOs) and MU1R forms (from authorized institution users and federal agency users) to comply with the information registration requirements of the SAFE Act and Regulation G.[28] MLOs must register annually (*i.e.,* renewal) with the CFPB through the Federal Registry and obtain a unique identifier.

To conduct FBI background checks for MLOs or identity verification for authorized institution users, only the relevant and necessary information, as prescribed by FBI and NIST policies, is collected for this purpose. Information collected for the purpose of identity verification retained in NMLSR and access to this data is controlled through access controls granted to authorized CFPB users.

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 records collected and maintained within NMLSR are retained for five years after an individual's or an institution's NMLSR account status becomes inactive in accordance with the applicable CFPB Records Schedule DAA-0587-2021-0001.

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

Privacy Risk: There is a risk that more information than needed may be collected.

Mitigation: The Federal Registry only collects information that is required for MLO registration under the SAFE Act and its implementing Regulation G using established MU4R and MU1R forms. Furthermore, the Federal Registry generally only publishes and shares information as specified in the SAFE Act and Regulation G to advance the consumer protection objectives, and other applicable state and Federal laws.

[28] *See, e.g.,* 12 C.F.R. 1007.103(d) and (e).

Certain information is collected for the purpose of conducting the FBI background check but is not published on the public CSBS Consumer Access Portal.[29]

3. Uses of Information

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

The Federal Registry collects PII[30] about MLOs, authorized institution users acting on behalf of a covered financial institution, and authorized federal users. Information in the Federal Registry is used to create a central repository to support the oversight and regulation of MLOs and to provide consumers with specific free information about MLOs through a public facing website.

In general, PII in the Federal Registry is used:

- To identify an individual acting as an MLO, create a unique account, and issue an NMLSR ID (unique identifier) for each MLO (through the registration process);
- To communicate with MLOs regarding their federal registration, and system users regarding system functionality;
- By the federal agencies in supervisory roles with respect to the covered financial institution, or in connection with any enforcement or disciplinary proceedings or complaint-related inquiries concerning an MLO;
- By covered financial institutions that employ MLOs as necessary for registering employees in the Federal Registry, for taking disciplinary actions or making employment decisions, for complying with applicable state and Federal law; and
- As a security measure to verify user identity and ensure the user has control over the MLO's account.

Additionally, the Federal Registry collects PII about authorized institution and authorized federal users to grant them access to the Federal Registry as part of their official duties.

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

[29] https://mortgage.nationwidelicensingsystem.org/Pages/default.aspx

[30] PII is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to an individual's identity." OMB, Circular No. A-130, Managing Information as a Strategic Resource, at Appendix II, (July 28, 2016).

MLO information within the Federal Registry is accessible and used by CFPB Staff for both routine and emerging business needs. Routinely, CFPB's Supervision Division accesses Federal Registry data in order to perform risk assessment analyses that inform the prioritization and selection of Supervision examination events that will be conducted by examiners. In these activities, NMLSR data is shared with both data/operations analysts and limited numbers of examiners.

Federal Registry data is also used for a variety of ad-hoc purposes across different offices and divisions throughout the CFPB to contribute to the Bureau's data-driven decision making and research activities. For example, the Offices of Research and Markets perform research projects and risk assessment/monitoring activities in response to executive priorities, external events (*e.g.*, Congressional inquiries, events in the financial marketplace) or intergovernmental initiatives for which the Federal Registry data is a helpful input. The Office of Regulations may also use the Federal Registry information to inform rulemaking activities.

The Enforcement Division also uses Federal Registry data as an input to investigation-specific needs. There are also cases where limited Federal Registry data is shared with CFPB Staff in the Operations Division, including the Office of Human Capital, Office of Technology & Innovation, and the Office of Finance and Procurement for the purpose of conducting administrative operations functions such as cybersecurity reviews (which include contractor resources), personnel reviews, and ensuring contractual obligations between CFPB and CSBS are met.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that the information may be used for unauthorized purposes by unauthorized users.

Mitigation: CFPB mitigates the risks that the information may be used for unauthorized purposes by implementing user role-based access controls within the system to ensure only authorized staff with need to know have access to the information. As stated above, the Federal Registry only uses and shares information to advance the consumer protection objectives of the SAFE Act and its implementing Regulation G, and other applicable state and Federal laws. Access to the nonpublic information in the Federal Registry must be approved at the institutional level and is restricted to registration of MLOs. The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

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 its rulemakings, this PIA, and applicable SORN(s). As noted above, the Federal Registry uses two standard MU electronic forms. The MU4R collects registration and account information from individual MLOs. The MU1R is used to establish Federal Registry accounts for covered financial institutions and to designate those institutions' administrators. In addition, covered financial institutions can upload information to the Federal Registry using a batch upload process that contains the same information from the MU forms.

As part of the registration process, MLOs are presented with Terms of Use before submitting the appropriate form which includes a Privacy Act Statement outlining how their information will or may be shared. Regulation G requires covered financial institutions that employ MLOs to adopt and follow written policies and procedures to ensure compliance with the registration process, including confirming the accuracy of MLO registrations, including updates and renewals.[31]

MLOs and covered financial institution employees can access, manage, and update most of the MLO and covered financial institution information in the Federal Registry via their account access. Additionally, CFPB offers individuals, through the Privacy Act of 1974[32] and CFPB's Privacy Act regulations at 12 C.F.R. 1070.50 *et seq.*, a means to access, amend, or correct their records.

Individuals may submit a Privacy Act request in writing in accordance with instructions appearing in the Bureau's Disclosure of Records and Information Rules, promulgated at 12 C.F.R. 1070.50 *et seq.* to: Chief Privacy Officer, Consumer Financial Protection Bureau, 1700 G Street, NW, Washington, D.C. 20552.

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.

The MLO must attest to the accuracy of the information submitted to the Registry; must authorize the Registry and the institution to obtain information related to any administrative, civil, or criminal action to which the employee is a party; and must authorize the Registry to make certain information available to the public.

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

[31] 12 C.F.R. 1007.104.

[32] 5 U.S.C. § 552a.

All users are able to access their account information. Additionally, MLOs and authorized institution users can access, manage, and update most of the MLO and covered financial institution information in the Federal Registry. CFPB also offers a means through the Privacy Act of 1974 and CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 *et seq.*, for individuals to access, amend, or correct their records.

Therefore, individuals may seek to access or correct their information maintained in the Federal Registry through the CFPB's Freedom of Information Act (FOIA) Office in writing in accordance with the Bureau's Disclosure of Records and Information Rules, Subpart E-Privacy Act [33] 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.

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that individuals will not be able to decline to provide certain information in the Federal Registry system. For example, an MLO is required to submit to the Federal Registry the MLO's name and any other names used.

Mitigation: This risk is acceptable because individuals acting as MLOs are required to provide information related to the registration of MLOs.[34] Also, their participation is in a business capacity which reduces their risk as individuals.

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.

The Federal Registry is a web-based system where information about registered MLOs may be accessible to entities external to the CFPB, such as authorized federal agencies, authorized institution users, and consumers.

The following information is made available to consumers through CSBS' Consumer Access Portal after MLOs grant authorization to CFPB during the registration or renewal process:[35]

- MLO name (first, last, middle) and former or other names or aliases, if applicable;

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

[34] 12 C.F.R. 1007.103(d)(1)(i)(A).

[35] 12 C.F.R. 1007.103 (d)(2)(iii).

- Current or most recent covered financial institution employer and/or financial services-related employment and history for the past 10 years including employer names, dates, and addresses;
- Principal business location address and business contact information including business phone/work phone number;
- History of financial services-related civil judicial actions, customer-initiated arbitrations, dismissals with settlements, and certain other judicial findings (other than actions dismissed without a settlement agreement), certain regulatory and disciplinary actions or orders, and revocations or suspensions of the employee's authorization to act as an attorney, accountant, or state or Federal contractor;
- Convictions of any criminal offense involving dishonesty, breach of trust, or money laundering against the employee or organizations controlled by the employee, or agreements to enter into a pretrial diversion or similar program in connection with the prosecution for such offense(s);
- Federal registration status (*e.g.*, active, or inactive and who they are authorized to represent); and
- NMLSR ID (unique identifier).

Authorized institution users have more extensive access to the MLO information, given their role and responsibilities to enter this information into the Federal Registry. They have the ability to view and generate reports related to the MLOs that include (see Appendix A for the various types of reports):

- Information submitted on the MLO's MU4R form (excluding SSNs and DOB);
- MLO's current registration status;
- Background checking including the request status of the request (*i.e.*, closed, expired, pending fingerprint, processing fingerprint, processing name check); and
- Latest information for the employment between the MLO and covered financial institution, if any.

CFPB and authorized federal users may have access to the non-public MLO information contained in the Federal Registry to the extent that such MLOs are subject to their exclusive or shared jurisdiction. CFPB has access to all data provided on the MU1R and MU4R forms, however no CFPB employee can view an individual's home phone number, information submitted as part of a background check, or the full SSN. The CFPB only shares information with those that have a need to know and in accordance with all laws, regulations, policies, and applicable SORN(s).

The SAFE Act protects the confidentiality of information about federally registered MLOs appearing within the Federal Registry when such information is shared between state and Federal regulatory officials with mortgage or financial services industry oversight authority.[36] Before disclosing non-public PII about MLOs (*i.e.*, information not accessible through the Consumer Access Portal) from any record in the Federal Registry to a third party, the disclosing agency must alert CFPB and the regulating agency with authority for the institution to which the record relates.

The Federal Registry also provides ad-hoc reporting services to supplement the reporting and download capabilities. Ad hoc reports are available (for a fee) only to authorized recipients and come in a variety of formats and contain information relevant to the requesting institution or agency only. CSBS works with the requesting financial institution on any reporting requirements and provides the reports directly to the requesting financial institution.

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

Authorized users from federal agencies, MLOs, authorized institution users acting on behalf of the covered financial institutions are allowed access by CFPB. Controls include the fact that relevant individuals are carefully screened before receiving access, have a need to know the information for legitimate purposes on behalf of their organizations, receive training in proper use of the data, and have read only access to the public information database on MLOs. Agencies are also responsible for developing internal policies and procedures for access and for ensuring that established rules of behavior are in place and enforced. Access for contractor employees who manage the system is controlled by the contractor, but the same standards are enforced as for CFPB employees.

The Federal Registry requires each user of non-public information to have a logon ID and password, and to sign a user agreement prior to access. Additionally, authorized federal agency users with access to multiple federal agency-regulated MLO records must have two-factor authentication. Privileged Users, a subset of authorized agency users who operate and maintain the system, are subject to additional requirements before being granted access to privileged functions.

MLOs and covered authorized institution users seeking access to the Federal Registry must request that an account be set up as. Once an account is established, information access is granted based on defined user roles, as applicable.

[36] 12 U.S.C. § 5111.

The Federal Registry also employs automated mechanisms to support the management of user accounts. These mechanisms automatically terminate temporary and emergency accounts after 24 hours. The Federal Registry automatically disables inactive accounts after:

- 120 days of inactivity for Privileged Users; or
- 15 months of inactivity in the system for MLOs.

Accounts are moved into a "Registered-Inactive" status when:

- The MLO fails to renew their registration within the renewal time; or
- The MLO's employment with the covered financial institution is terminated and no other employment(s) remain.

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

Privacy Risk: There is a risk that information maintained within NMLSR may be accessed by unauthorized individuals who do not have a need to know or used in a manner that is inconsistent with the purpose for collection.

Mitigation: To mitigate this risk, the system is subject to the Federal Information Security Modernization Act (FISMA), 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 system. CFPB Staff are responsible for granting access to and will terminate access for CFPB Staff in accordance with all policies and protocols.

Finally, NMLSR generates audit logs of user activity, including external users, to monitor unusual system behavior. Audit logs track when users are logged onto the system, who views which records, who uploads documents to a matter record, and how records are used within the system (*e.g.*, unauthorized creation, system configurations). Any evidence of misuse may result in the termination of the user account.

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,[37] the Right to Financial Privacy Act,[38] and the E-Government Act of 2002, Section 208.[39] To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopted the Fair Information Practice Principles (FIPPs) as the framework for its privacy policy.[40] 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 to ensure compliance with all laws, regulations, and policy requirements.

The CFPB adheres to the Office of Management and Budget (OMB) privacy-related guidance [41] and applies the National Institute of Standards and Technology (NIST) Risk Management Framework for information technology systems, applications, solutions, and services.[42] The NIST RMF identifies processes for the identification of NIST SP-800-53 security and privacy controls and continuous monitoring of controls to ensure on-going compliance.[43]

The Federal Registry, along with the NMLSR has obtained an Authority to Operate (ATO) from the CFPB's authorizing official. In addition, the Federal Registry receives an annual FISMA Assessment by an independent third party to maintain that ATO. All controls are aligned to the FISMA requirements.

Certain authorized institution users who are designated to perform administrative functions on behalf of the federally supervised entity require access to CHRI of MLOs as part of their duties. As such, these individuals are required by the FBI to undergo identity verification. All CFPB Staff (*e.g.*, federal employees and contractors) with access to CFPB information and systems are subject to the same federal laws, regulations, and policies while working at the CFPB and proceed through the same background investigations for suitability and security clearance determinations. This

---

[37] 5 U.S.C.§ 552a.

[38] 12 U.S.C. §§ 3401-3423.

[39] 44 U.S.C. § 101.

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

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

[42] *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.

[43] *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.

ensures individuals supporting the CFPB are deemed reliable, trustworthy, and suitable for the role they will fulfill.

In addition, the CFPB employs role-based access controls. to ensure users only have access to the system and/or information necessary and relevant to their assigned duties. It is important to note that not all information (including PII) in the Federal Registry is available to all system users, rather, only categories of user roles based on need to know. System administrators provide access based on the user's role within the CFPB upon submission of a signed request for access approval from their supervisor. Individuals who no longer require access have their credential removed from the system.

Agencies grant their authorized users access as necessary to carry out official duties. Agencies are also responsible for developing internal policies and procedures for access and for ensuring that established rules of behavior are in place and enforced. Access for contractor employees who manage the system is controlled by the contractor, but the same standards are enforced as for CFPB employees. The Federal Registry requires each user of non-public information to have a logon ID and password, and to sign a user terms of agreement prior to access. Additionally, authorized agency users with access to multiple federal agency-regulated MLO records must have a two-factor authentication. Privileged Users, a subset of authorized agency users who operate and maintain the system, are subject to additional requirements before being granted access to privileged functions.

The system uses automated mechanisms to audit account creation, modification, disabling, and user session termination actions. In addition, audit reviews are completed each month to ensure that user access, roles, and disabling mechanisms follow documented processes. All data exchanges take place over encrypted data communication networks, and private networks and encryption technologies are used during the transfer of information. Additionally, the NMLSR Consumer Access Portal is physically separated from the Federal Registry. This ensures that non-public information is not inadvertently disclosed to the public via the NMLSR Consumer Access Portal. Rather, information maintained in the Federal Registry (and NMLSR) that is considered public information is tagged/coded appropriately to automate the sharing of information between the Federal Registry and the NMLSR Consumer Access Portal.

In addition to the system’s technical capabilities, Regulation G requires covered financial institutions that employ MLOs to adopt and follow written policies and procedures to ensure

compliance with the registration process, including confirming the accuracy of MLO registrations, including updates and renewals.[44]

CSBS is responsible for managing the Federal Registry and have established an internal incident response capability and monitor event logs for the system. They will notify CFPB if a data breach is discovered. The CFPB requires all employees to complete privacy and security training. CSBS employees, who also operate the Federal Registry, are required to complete annual privacy and security training and to execute a non-disclosure agreement before being granted access to the system.

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 within thirty days and annually thereafter. The Privacy Training ensures that CFPB 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. CFPB and CSBS Staff are required to complete privacy and security training annually, and to execute a non-disclosure agreement prior to being granted access to the system.

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 before onboarding. 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" 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).

[44] 12 C.F.R. 1007.104.

This ensures the CFPB maintains a secure operating environment and protects our systems against potential external threats.

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

Privacy Risk: There is a risk that unauthorized users may access the Federal Registry or information maintained therein.

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 Federal Registry. For example, internal access to the Federal Registry is limited to CFPB Staff that have a need to know. As noted above, CFPB Staff cannot obtain access without being granted access by system administrators. The Federal Registry also employs automated mechanisms to support the management of user accounts. These mechanisms automatically terminate temporary and emergency accounts after 24 hours.

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 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. CFPB Staff are required to review and sign the CFPB's "Acceptable Use of CFPB Technology Resources Policy" 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 review audit logs of the system and applications identified herein to monitor for unusual behavior (*e.g.*, disabling 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 in violation of CFPB policy, system access may be revoked. If there is evidence of potential misconduct, the incident will be referred to the appropriate Bureau office for investigation and further review. CFPB Staff will be disciplined accordingly, which could include adverse actions or removal from the CFPB.

Privacy Risk: In the event of a privacy breach, among others, there is a potential risk of embarrassment or loss of reputation to both the individual and CFPB. A privacy breach may result in MLOs suffering financial harm because of identity theft.

Mitigation: CFPB mitigates this risk of privacy breaches by enforcing access controls to limit the number of individuals (at the federal agencies and covered financial institutions) who have access

to the non-public data through a system of two-factor authentication. CFPB Staff are also trained on how to handle potential breaches to minimize negative impacts. Additionally, covered financial institutions may have special information access controls in place to minimize risk of privacy breach through the assignment of roles and responsibilities.

APPENDIX A – FEDERAL REGISTRY REPORTS AVAILABLE TO AUTHORIZED USERS AT A COVERED FINANCIAL INSTITUTION

Report Title	Report Description
Federal Criminal Background Check Status Report	Displays the current Criminal Background Check request status for mortgage loan originators pending confirmation of employment with the covered financial institution.
Individual Roster Report	Lists the mortgage loan originators associated with the covered financial institution, the mortgage loan originator's current registration status, the Criminal Background Check request status for the most recent request and the latest information for the employment between the MLO and the covered financial institution, if any.
MU4R Detail Report	Displays expanded data (excluding SSN and DOB) from the most recently submitted MU4R. Also includes the mortgage loan originator's current registration status, the Criminal Background Check request status, and the latest information for the employment between the mortgage loan originator and the covered financial institution, if any.

APPENDIX B - NMLSR CONSUMER ACCESS PORTAL

The SAFE Act and its implementing Regulation G require that consumers be provided with easily accessible information, at no cost and through electronic media, regarding the employment history of, and publicly adjudicated disciplinary and enforcement actions against MLOs.[45] The NMLSR Consumer Access Portal meets this requirement by providing, among other things, the public with the following Federal Registry information[46]:

- MLO name (first, last, middle) and former or other names or aliases, if applicable;
- Current or most recent covered financial institution employer and/or financial services-related employment and history for the past ten (10) years including employer names, dates, and addresses;
- Principal business location address and business contact information including business phone/work phone number;
- History of financial services-related civil judicial actions, customer-initiated arbitrations, dismissals with settlements, and certain other judicial findings (other than actions dismissed without a settlement agreement), certain regulatory and disciplinary actions or orders, and revocations or suspensions of the employee's authorization to act as an attorney, accountant, or state or Federal contractor;
- Convictions of any criminal offense involving dishonesty, breach of trust, or money laundering against the employee or organizations controlled by the employee, or agreements to enter into a pretrial diversion or similar program in connection with the prosecution for such offense(s);
- Federal registration status (e.g., active, or inactive and who they are authorized to represent);
- NMLSR ID (unique identifier).

Information in the NMLSR Consumer Access Portal is refreshed on a nightly basis. The information displayed will be viewable for five years after the MLO record becomes "inactive," after which it will no longer appear on the NMLSR Consumer Access Portal website but will remain in the Federal Registry. If the MLO "re-activates," the information will be viewable again.

---

[45] *See, e.g.*, 12 U.S.C. § 5101; 12 C.F.R. 1007.103(d)(2)(iii).

[46] There is more information posted publicly based on information from state regulators. Appendix B is only listing the Federal Registry data that is made public. The CFPB also posts CFPB public enforcement actions to the NMLSR if the respondent has an NMLS user account.

Document Control

Approval

_____

Chris Chilbert
Chief Information Officer

_____

Kathryn Fong
Chief Privacy Officer

_____

Katelyn Sellers
Product/Business Owner

Original, signed document on file with the CFPB Privacy Office.

Change Control

Version	Summary of material changes	Pages affected	Date of change
1.0	Original 2012 publication.	All	September 2012
2.0	Updated to include use of third-party vendor to conduct background check of MLOs; identify additional individuals about whom the information pertains (*e.g.*, POCs and users designated to perform administrative functions); identify the information collected for identity verification.	All	January 2026
3.0	General updates.	All	February 2026