Small Business Lending System v.1

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Facilitating enforcement of fair lending laws; enabling communities, governmental entities, and creditors to identify business and community development needs and opportunities of women-owned, minority-owned, and small businesses.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Generally applicable: Appropriate opportunities for notice, consent, access, and redress.

Overview

Section 1071 of the Consumer Protection Act of 2010, title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law No. 111-203, 124 Stat. 1376, 2004 (2010) amended the Equal Credit Opportunity Act (ECOA), 15 U.S.C. 1691 *et. seq.* (hereinafter Section 1071) to require covered financial institutions to collect data regarding applications for credit for women-owned, minority-owned, and small businesses and report it to the Consumer Financial Protection Bureau (CFPB). Section 1071's statutory purposes are to (1) facilitate enforcement of fair lending laws, and (2) enable communities, governmental entities, and creditors to identify business and community development needs and opportunities of women-owned, minority-owned, and small businesses.

Section 1071 specifies data that covered financial institutions are required to collect from small business applicants and report to the CFPB. It also provides authority for the CFPB to require additional data that it determines would fulfill Section 1071's statutory purposes. Section 1071 further provides that financial institutions may not include the personally identifiable information (PII) of applicants as part of the data collection disclosed to CFPB.

Pursuant to ECOA, the CFPB issued the Small Business Lending Rule, codified as subpart B to Regulation B, 12 C.F.R. 1002.101 et seq., which implements the small business lending data collection requirements set forth in Section 1071[1]. Regulation B prescribes rules for covered financial institutions to follow when collecting and compiling data related to small business lending as required by Section 1071.

The data that will be collected by covered financial institutions from small business credit applicants includes the type of credit being applied for; the credit purpose; and the amount applied for; census tract based on an address or location provided by the applicant; gross annual revenue for the preceding fiscal year; the 3-digit North American Industry Classification System (NAICS) code for the applicant; the number of workers that the applicant has; the applicant's time in business; and the number of principal owners the applicant has.

[1] See Small Business Lending under the Equal Credit Opportunity Act (Regulation B) final rule published here: https://www.federalregister.gov/documents/2023/05/31/2023-07230/small-business-lending-under-the-equal-credit-opportunity-act-regulation-b

Moreover, covered financial institutions must collect and report certain demographic information about the applicant and its principal owners. The demographic data collected will include whether the applicant is a minority-owned, women-owned or LGBTQI+-owned business, and the ethnicity, race, and sex/gender of the applicant's principal owners.

Finally, covered financial institutions must report data points that are provided solely by the financial institution. For all applications this data includes: a unique identifier for each application for or extension of credit; the application date; the application method (that is, the means by which the applicant submitted the application); the application recipient (that is, whether the financial institution or its affiliate received the application directly, or whether it was received by the financial institution via a third party); the action taken by the financial institution on the application; and the action taken date. For denied applications, there is also a data point for denial reasons. For applications that are approved, additional data is required including the amount originated or approved, and pricing information.

The CFPB created the Small Business Lending system (herein referred to as the SBL system) built within CFPB's Amazon Web Services (AWS)[2] environment to collect small business lending data from covered financial institutions, as required by Section 1071. Prior to full deployment of the system, the CFPB is conducting beta-testing activities. During the beta-testing phase, the CFPB will test the functionalities of the SBL system with volunteer participants from covered financial institutions. During the beta-testing activities, the volunteer user or point of contact (POC) from covered financial institutions is instructed to only submit fake data through the SBL system; the CFPB is not collecting any real application data during this phase. The CFPB will provide simulated datasets to be used for this purpose. Any information provided to the CFPB during beta-testing will only be used for testing purposes. The CFPB is conducting this PIA to document and assess privacy risks associated with the limited collection of PII from the volunteer user or POC during the beta testing activities.

To access the SBL system for testing, the volunteer user or POC must first visit Login.gov, which is owned and operated by the General Services Administration (GSA)[3] to create an account. The user or POC must provide their full name and email to create an account with Login.gov; their information is then shared with and collected by the SBL system to authenticate the account and

[2] Please see: https://www.consumerfinance.gov/privacy/privacy-impact-assessments

[3] For more information on Login.gov, please visit: https://login.gov/what-is-login

grant access to the system. The volunteer user or POC is then directed to the CFPB Regulatory Technology Home web application[4] where they create a User Profile. The SBL system collects the volunteer user's or POC's full name, business email address, phone number, and mailing address, along with other information related to the covered financial institutions, to create the User Profile. Once the User Profile is created, the volunteer user or POC is able to test the submission capabilities in the SBL system by uploading and providing fake data through the system. The CFPB testing team receives the data and validates that the submission process is functioning correctly.

The information collected by the SBL system from the volunteer user or POC for the purpose of authorizing access to the SBL system and creating a User Profile within the system for beta-testing are covered by SORN CFPB.014, Direct Registration and User Management System (DRUMS).[5] The Office of Management and Budget (OMB) has approved the information collections contained in Regulation B under the Paperwork Reduction Act provisions, 44 U.S.C. 3501 et seq. and assigned the information collection number OMB Control No. 3170-0013.

Before the system begins to receive real SBL data from covered financial institutions per the SBL final rule, the CFPB will update this PIA. As discussed in the SBL final rule, the CFPB will make available to the public, on an annual basis, the application-level data submitted to it by financial institutions, subject to modifications or deletions made by the CFPB, to advance privacy interests. The CFPB does not anticipate that it can carry out the necessary analysis of pre-publication modifications and deletions without at least one full year of application-level data. The CFPB intends to further engage with stakeholders on the issue of data publication before it resolves on a particular approach to protecting privacy interests through modifications and deletions. Finally, the CFPB anticipates publishing select aggregate data—*i.e.,* data that does not include application-level information—before it publishes application-level data.

Privacy Risk Analysis

The primary risks associated with PII covered by this PIA are related to the following:

- Data minimization; and

[4] CFPB Regulatory Technology Home web application

[5] Please see: https://www.consumerfinance.gov/privacy/system-records-notices

- Security.

Data Minimization

Covered financial institutions are instructed to only provide fake data during the beta-testing activities; no real application data should be provided to the CFPB during this phase. Furthermore, the CFPB provides simulated data to financial institutions to upload during testing. However, there is a risk that financial institutions volunteer user or POC may inadvertently upload their own file that contains PII. The CFPB mitigates this risk by only using the information received for testing purposes. Additionally, information is not shared outside of the SBL system testing team. Furthermore, the volunteer user or POC can request for removal of any data they submit to the system.

Security

The CFPB takes measures to mitigate and address any risks to the security of data it receives, consistent with the guidance and standards set for federal information security and privacy programs. As such, security and privacy were considered during the design and development of the system to ensure that data collection and use practices had appropriate controls built in. The CFPB provides its employees and contractors with appropriate privacy and security training to ensure information is used and secured appropriately, and access controls are implemented and managed by the system owner to ensure only those with authorized access can use the data.

The technical, physical, and administrative controls implemented are appropriate for the testing of the SBL system.

Privacy Risk Management

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

Once the volunteer user or POC accesses the SBL system though Login.gov, they are directed to create the User Profile within the SBL system. This information includes full name, business email, phone number, and mailing address. However, for purposes of beta-testing, any information submitted beyond user or POC business contact information, including information

regarding small business loan application filing, is only fake data. No information related to actual applicants or individuals associated with applicants is collected by the CFPB during beta-testing activities.

After full deployment, the CFPB will collect data from covered financial institutions about the institution itself and details about small business loan applications, including certain protected demographic information of applicants for credit. These data will be submitted by users or POCs into the SBL system.

2. Describe CFPB's objective for the information.

During beta-testing activities, the CFPB uses the information from the volunteer user or POC to register a financial institution within the SBL system. Any information collected during the beta-testing activities is only used to test the functionality of the SBL system.

After full deployment, information collected by the SBL system will support and facilitate the enforcement of fair lending laws by the CFPB and other agencies. Additionally, it will enable communities, governmental entities, and creditors to identify business and community development needs and opportunities of women-owned, minority-owned, and small businesses.

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

Information collected during beta testing-activities is only used by CFPB to create user profiles and test the functionality of the system. It will not be shared with any third parties.

After full deployment, information collected by the SBL system may be shared with other federal or state agencies, as authorized, and with whom CFPB has entered into agreements regarding the sharing and use of data.

4. Describe what opportunities, if any, individuals to whom the information pertains have to (a) receive notice regarding the CFPB's use of the information; (b) consent to such use; (c)

access the information that pertains to them; or (d) obtain redress.

The CFPB provides notice to the user or POC prior to the beta-testing activities, and on the User Profile page, on how their information will be used, and participation in these activities is voluntary. As applicable, the CFPB allows individuals to request access and amend their PII per the Privacy Act of 1974, 5 U.S.C. § 552a and the CFPB's Privacy Act regulations at 12 C.F.R. § 1070.50 et seq. Information about Privacy Act requests is published in the associated SORNs and on the CFPB's website. Individuals may also file a request for information under the Freedom of Information Act.

5. Explain the standards and relevant controls that govern the CFPB's—or any third party contractor(s) acting on behalf of the CFPB—collection, use, disclosure, retention, or disposal of information.

The CFPB complies with the Right to Financial Privacy Act and the E-Government Act of 2002; adopts Office of Management and Budget privacy-related guidance as best practice; and applies National Institute of Standards and Technology risk management processes for implementing privacy controls. The CFPB also uses the following technical and administrative controls to secure the information and create accountability for CFPB's appropriate collection, use, disclosure, and retention of the information:

- Audit logs and reviews to ensure that only authorized individuals are able to access and use any data within the system.
- CFPB general awareness and role-based privacy training to ensure that those who have access to PII understanding their responsibilities.
- CFPB Privacy Breach Response and Recovery Plan to identify and address a suspected breach of PII.
- Compliance with CFPB cybersecurity policy and procedures to ensure the confidentiality, integrity, and availability of data within the system.
- Data quality and integrity checks to ensure that the data used by CFPB is accurate and used for the purpose for which it was collected.
- Extract logging and 90-day reviews to identify user behavior around particular events, such as changes in the data, warnings, or errors that are unexpected.

- Policy and Standard Operating Procedures to establish guardrails for the collect and use of data within the system.
- Role-based access controls: The CFPB is responsible for assigning and maintaining roles and permissions within the system based on an individual's role within the organization and as approved by Cybersecurity. The following lists examples of the roles and responsibilities within the system:
    - SBL Users – Members of financial institutions who submit fake data to test the functionality of the SBL system
    - CFPB Admin – Members of the CFPB who have access to the authorization console
        - Read and Write – backend developer for system operation and maintenance.
- The CFPB does not currently have a records schedule for the SBL system. The records contained within the system are considered unscheduled and will be maintained as permanent until there is an approved records schedule for SBL.
- Personnel security, including background checks. The CFPB may use contractors to help support the collection, use, disclosure, or retention of information covered by this PIA, and those contractors are subject to similar controls. Other requirements placed on contractors may include training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations.

As a result of conducting this initial PIA, the CFPB established the Privacy Notice at the point of collection of beta-testing data to ensure that SBL volunteer users or POCs, on behalf of covered financial institutions, understand the purpose of the collection and uses of the data being submitted for beta testing.

6. Discuss the role of third party(ies) that collaborate or partner with the CFPB, if any. Identify any controls used to protect against inappropriate collection, use, disclosure, or retention of information. (This does not include third parties acting on behalf

of the CFPB, e.g., government contractors discussed in Question 5.)

The CFPB built and manages the SBL system within its AWS environment[6].

[6] Please see the CFPB Amazon Web Services (AWS) Alto General Support System PIA found at: https://files.consumerfinance.gov/f/documents/cfpb_aws-alto_pia_2023-01.pdf

Document control

Approval

Irfan Malik

Digitally signed by Irfan Malik
Date: 2024.07.08 13:13:11 -04'00'

Irfan Malik, delegate for Chris Chilbert

Chief Information Officer

Date

KATHRYN FONG

Digitally signed by KATHRYN FONG
Date: 2024.07.08 13:15:52 -04'00'

Kathryn Fong

Chief Privacy Officer

Date

MONICA SHELTON

Digitally signed by MONICA SHELTON
Date: 2024.07.08 12:38:26 -04'00'

Monica Shelton

Project/System Owner

Date

Change control

Version	Summary of material changes	Pages affected	Date of change
1.0	Initial publication	All	July 2024