PRIVACY IMPACT ASSESSMENT—JANUARY 2024

Legal Technology Support Team (LTST) v.2

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Maintain records pertaining to investigations, enforcement, and litigation activities.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	When applicable: Appropriate opportunities for notice, consent access, and redress.

Consumer Financial Protection Bureau

Overview

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

In carrying out its statutory mandate, CFPB manages a variety of legal responsibilities. This includes conducting investigations and analyses on financial services and products offered by financial institutions and brings civil and administrative law enforcement actions against financial institutions and individuals subject to its authority. The CFPB also defends itself in litigation resulting from those enforcement activities, as well as in litigation arising in personnel actions, contracts, and actions subject to the Freedom of Information Act (FOIA).

The CFPB employs the Legal Technology Support Team (LTST), which hosts and provides end-user support with a suite of applications, systems, and processes to manage these legal activities. LTST primarily allows CFPB to effectively collect, store, process, transmit, and maintain critical information related to CFPB investigations, litigation, and enforcement processes. LTST's application suite is comprised of customized commercial off-the-shelf (COTS) computer hardware, software, and cloud-based solutions (on-premises or vendor-owned). These tools help LTST manage case activities, secure information transfers (if required), and communicate between several CFPB programs. LTST includes tools that enable CFPB programs to identify, collect, review, make redactions to, and produce documentation as part of the litigation lifecycle, and secure file transfer mechanisms that enable information to be safely shared with external entities. Other tools provide CFPB with the ability to conduct secure virtual meetings and depositions with authorized individuals involved in investigations, litigation, or examinations.

As part of this support, LTST facilitates the collection, use, maintenance, and sharing of information, including personally identifiable information (PII). This PII may include contact information that is collected from expert witnesses, paralegals, opposing counsel, defendants, courts, or others who may have information or play a role in an investigation, enforcement, or litigation activity. PII is collected directly from individuals and companies that are the subjects of investigation, enforcement, or litigation action, or third-party legal stakeholders associated with the litigation action. PII is also collected from third parties, such as from existing federal databases, other agencies responsible for related regulatory functions, or from publicly available sources such as internet searches and publicly available data sources. LTST may also collect

information related to CFPB system users for account registration and access purposes, which includes authorized CFPB employees and contractors.

While LTST tools are primarily used to support CFPB legal activities, some of the tools can be used to provide limited internal project support for other CFPB operations, such as consumer response efforts, rulemaking reviews, and hiring support. For example, the document processing and redaction tool may be used by the Office of Human Capital (OHC) to redact PII from resumes prior to an internal review, public comments received during draft rulemaking, records requested under FOIA that may require redaction prior to release. LTST also provides the capability of collecting, maintaining, sharing, or redacting PII based upon the direction and requirements of the program requesting support. For example, if a program requests to use LTST tools to securely share information related to CFPB matter, LTST provides a secure file transfer application or an encrypted thumb drive/CD to meet the request.

The initial collection, processing, and subsequent sharing of PII is subject to program and privacy compliance requirements as described within their associated Privacy Impact Assessments (PIA) and System of Records Notices (SORNs) identified below and in accordance with CFPB's legal authority under the Dodd-Frank Act LTST tools do not enable any new collections or uses of PII, instead these tools provide a secure method to collect data and process data as authorized by CFPB rules. The type of PII and method of collection may vary depending on the need of a particular CFPB program or end user, such as the nature of the investigation, enforcement, or litigation, or other activity requested by a CFPB program. However, CFPB only collects and maintains PII consistent with its legal authority under the Dodd-Frank Act, and any use of LTST to collect or process PII by CFPB programs is covered by separate, program-specific and system specific PIAs and SORNs, as appropriate. For example, in cases where LTST is used for redacting information, the information is first sent internally to LTST and tools are used to redact the information requested. The redacted information is then returned to the CFPB program for use. This information is not stored by LTST.

CFPB is publishing this PIA to document to update the name change of the prior Litigation and Investigation Support Toolset PIA to Legal Technology Support Team (LTST) PIA and to document new capabilities of LTST. This PIA also assesses the collection and use of PII that supports CFPB's investigation, enforcement, litigation, and other CFPB program activities through LTST and its suite of applications. It also addresses the associated privacy risks, including risks associated with maintaining information in a third-party cloud environment, and how CFPB mitigates those risks. This updated PIA will replace all previous versions.

As noted above, any other CFPB program uses of LTST products are covered under program specific PIAs such as the Supervision, Enforcement, and Fair Lending Data PIA, the Labor and Employee Relations System PIA, and the Freedom of Information Act (FOIA) and Privacy Act System (FOIAXpress) PIA[1].

The records pertaining to individuals related to investigations, enforcement, and litigation are accounted for in CFPB.004 Enforcement Database SORN and CFPB.018 Litigation Files SORN. Records that are used by LTST for tasks such as redaction are accounted for in related SORNs, such as the Freedom of Information Act (FOIA)/Privacy Act System SORN[2]. Records related to individual users of LTST are accounted for in CFPB.014 Direct Registration and User Management System SORN. LTST does not use any forms subject to the Paperwork Reduction Act (PRA) requirements. Any other program use of LTST or their suite of applications is covered by program-related SORNs and authorized by Sections 1012, 1021, 1051-54 of the Dodd-Frank Act.

Privacy Risk Analysis

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

- Purpose of Collection
- Individual Participation
- Security
- Accountability and Auditing.

Purpose of Collection

CFPB collects information from various sources, directly from individuals, from financial institutions, internally from CFPB programs that request services, and/or from other third-party sources. The amount and type of information that is collected is dependent on the nature and scope of the investigation, enforcement, litigation activity, or program request. There is a risk that CFPB could collect and maintain a large volume of PII and other sensitive information that is not necessary, or that it could use such information beyond proper investigative, enforcement, or litigation activity purposes. CFPB mitigates this risk by minimizing, to the extent practical, such collections, ensuring the collection of information to only what is relevant, and collecting

[1] CFPB PIAs are found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[2] CFPB SORNs are found at https://www.consumerfinance.gov/privacy/system-records-notices/.

necessary information related to each investigation or legal activity. LTST designs and configures its applications to collect PII according to the purposes governed by CFPB's legal authorities and regulations, and as required by the authorized program that uses LTST to collect and use PII. For internal requests to redact information, LTST follows applicable law and federal guidance when performing the activity. For example, LTST may only redact FOIA information under one of nine exemptions. In addition, when CFPB programs request LTST services, the LTST program managers follow the purpose and use specifications of data that pertains to that program.

Individual Participation

CFPB collects information directly from individuals, when practicable. However, due to the nature of investigation, enforcement, or litigation activities, it is not always possible, as CFPB may collect information from financial institutions or third parties that contain PII about individuals involved in a particular action. As such, individuals who suspect their information is incorrect can request to amend, remove, or update their records when feasible. Information about Privacy Act requests is available in CFPB.004 Enforcement Database SORN and CFPB.018 Litigation Files SORN and on the CFPB website[3]. Note that portions of the records in these SORNs are compiled for law enforcement purposes and may be exempt from disclosure under CFPB's Privacy Act regulations.

Security

The content and sensitivity of information held within the LTST data resources may be a target for unauthorized access and/or risk insider threats. As a suite of cloud-based and desktop tools, the use and sharing of information in LTST is secured by a third-party vendor. This kind of use and sharing of information introduces security risk. As a result, information within LTST's application suite is subject to the appropriate technical, physical, and administrative safeguards implemented to address these security risks, such as encryption for data maintained within the system, encryption of information uploaded into cloud-based and desktop tools, and the employment of multi-factor authentication and access safeguards to conduct virtual investigative proceedings. For example, LTST requires all team members to sign a Rules of Behavior (RoB) form as well as a Privileged User Access (PUA) form to determine the type of access required before authorized individuals gain access.

These security safeguards are put in place in order to control unauthorized access to sensitive information. National Institute of Standards and Technology (NIST) controls families, including Identification and Authentication (IA), Risk Assessment (RA), Access Controls (AC), and Systems

[3] Please see https://www.consumerfinance.gov/foia-requests/.

and Communications Protection (SC), are implemented to restrict access to information to only authorized CFPB staff and authorized external participants. Specific to cloud-based and desktop tools, only authorized CFPB staff, including contractors, may upload, access, share, or dispose of documentation within the tool. No third-party access to CFPB's data within the tool is authorized for any purposes. CFPB has appropriate technical safeguards and policies and procedures in place, which restrict access to PII collected through an investigation, enforcement action, or part of a litigation. Further, all tools managed within LTST are assessed by CFPB following the NIST Risk Management Framework (RMF) to ensure that each tool has the appropriate security and privacy controls in place prior to use. These controls are assessed using continuous monitoring practices to ensure control effectiveness.

Accountability and Auditing

The LTST environment consists of a diverse set of tools used to support CFPB's investigation, enforcement, litigation, and other program activities. PII is collected about subjects of CFPB's enforcement activities, expert witnesses, paralegals, opposing counsel, defendants, via FOIA requests, courts, etc. This leads to a risk that the PII that LTST maintains, collects, and utilizes for different purposes could be accessed inadvertently by an unauthorized individual. CFPB mitigates this risk through data access safeguards supported by role-based privacy training for individuals who handle the data. CFPB's RoB provide guidance and specific rules on the appropriate use of CFPB information systems for individuals granted access to LTST. Individuals must review, acknowledge, and sign that they understand CFPB's RoB. Individuals are also only authorized to receive the minimum access required to accomplish assigned core job functions. Individuals requiring privileged access must also receive system owner approval by completing a PUA before granting such access.

Additionally, both internal and independent auditors hold CFPB accountable for complying with CFPB's policies and procedures related to the processing of PII. LTST works with Cyber personnel to review and manage accountability as well as conduct audits to ensure individuals are using LTST tools correctly. CFPB is committed to taking swift and immediate action upon uncovering any violations of law, policies, and procedures.

The technical, physical, and administrative safeguards implemented to promote individual participation, minimization and accountability are appropriate and implemented within the LTST environment.

Privacy Risk Management

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

CFPB uses LTST to collect, maintain, and process PII that CFPB obtains as part of its investigation, enforcement, litigation activities, or by requests from CFPB programs. The type of PII may vary depending on the type of use, including investigation, enforcement, consumer response, rulemaking reviews, hiring support, litigation, and other internal program support as requested. CFPB also reviews collections of data within each LTST application to minimize the collection of PII to the greatest extent possible, while allowing CFPB to complete its objectives. The collection of PII by LTST is specific to the need and as authorized by the program leveraging LTST to collect and use PII. PII elements generally may include but are not limited to:

- Financial transaction data, including consumer transaction data;
- Narratives and other information in complaints filed through CFPB's Consumer Response database;[4]
- Banking records;
- Credit reports;
- Contracts;
- Employee records;
- First name and last name;
- Titles;
- Account and credit card numbers;
- Social Security Numbers;
- Tax Identification Numbers;
- Contact information, to include phone number, home addresses, and email addresses; and
- Date of birth.

[4] The Consumer Response System PIA is available at: https://files.consumerfinance.gov/f/2012/01/CFPB_PIA_Consumer-Response.pdf.

CFPB uses LTST to collect PII from the following sources:

- Subjects of CFPB's enforcement activities;
- Individuals and financial institutions with information that may be relevant to CFPB's investigations;
- Individuals or third parties that may be relevant to or involved in the disposition of legal proceedings;
- Individuals who are or were customers or individuals who have been solicited by covered institutions;
- Individuals who submit a FOIA request or a resume for employment consideration;
- CFPB employees and contractors;
- In-person hearings and depositions that may be conducted as part of the investigation, enforcement, or litigation process.

2. Describe CFPB's objective for the information.

CFPB collects, maintains, and processes PII with LTST to support CFPB program activities. For example, CFPB uses LTST to collect PII to support:

- Locating victims of violations of consumer financial protection statutes and regulations or assisting with redress;
- Uses of various tools and technologies for several programs, which may include Enforcement, FOIA, and the Legal Division;
- Defending against suits brought against CFPB;
- Gathering and storing information in a secure and forensically sound manner, including electronic and non-electronic (e.g., paper) information;
- Providing an anonymous online browser platform in support of CFPB's investigations of financial services and products marketed by financial entities online;
- Performing computer forensic analysis and processing;
- Analyzing, processing, formatting, and organizing electronically stored information for search, retrieval, review, correlation, flagging, and presentation;
- Processing and preparing information for use in desktop-based review or case management tools or on CFPB's network;

- Providing redaction capabilities to identify and remove PII from resumes for the OHC reviews, the names of individuals that submitted comments on draft rulemakings, or information covered by FOIA;
- Processing and preparing information for use in a cloud-based mobile application that enables remote and virtual depositions and hearings;
- Assisting in the production of information as required in litigation and for courtroom presentation;
- Providing cloud-based and desktop tools that allow sharing of documentation that may include PII with authorized opposing attorneys, paralegals, and expert witnesses. This sharing is an obligation consistent with the legal authorities that allow CFPB to conduct investigations, enforcement, and litigation. The cloud-based and desktop tools provide CFPB with the ability to restrict the sharing of information to the minimum necessary to facilitate proceedings; and
- Secure file transfer of documents to authorized external recipients.

LTST collects and uses the minimum PII to perform tasks as identified by CFPB's program. When a program needs to collect PII, CFPB will assess the purpose of the system and its use to collect, use, and store PII. This assessment is completed by a review of LTST's design documents to determine whether CFPB has an authorized purpose to collect and use the information, and to ensure that PII used is both relevant and necessary to its intended purpose. During such activities, CFPB may share relevant investigation, enforcement, or litigation related information with third parties, to include authorized opposing attorneys, paralegals, experts, and witnesses. Any use and sharing of information are compatible with the purpose of collection, and information is only shared pursuant to regulatory and statutory requirements and court rules, and in accordance with applicable SORNs.

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.

LTST utilizes a collection of tools and technologies for several programs, which may include Enforcement, FOIA, OHC, and the Legal Division. LTST collects the information, and goes on to provide the information to various program offices. Program offices have the authority to externally share the information collected by LTST. If program offices use LTST to share collected

information, LTST can be directed by that program office to facilitate the information sharing process. For example, LTST provides cloud-based and desktop tools that allow CFPB to share documentation with third parties during virtual hearings and depositions. LTST also provides access to state and federal agencies that CFPB has partnered with to enforce consumer financial laws. Access to shared data is limited to third parties authorized by CFPB. Moreover, sharing of PII is consistent with the routine uses as published within applicable CFPB SORNs.

CFPB may also share PII with external entities that are the subjects of an investigation or parties to litigation, and their legal representation. External sharing includes in-person and virtual hearings and depositions of individuals and expert witnesses, and opposing counsel. During in-person investigative processes, CFPB attorneys may present documentation relevant to the legal matter that may include PII of individuals involved in the matter. Sharing this documentation is a requirement of CFPB's investigative process, and other litigation processes. LTST provides CFPB with a secure method of sharing this information.

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.

Wherever required, CFPB provides notice to individuals about its policies regarding the use of information at the time information is collected. Given the broad collection of information from various sources, LTST notice may be provided in multiple formats. For information collected pursuant to a request for information from CFPB, notice is provided as part of the request (e.g., in a letter request, or in a document outlining the compulsory process request). For information collected from internal CFPB systems for internal investigations or the defense of suits brought against CFPB, staff are informed that the agency's computing systems are monitored, and that personal information may be collected at any time. Notice is provided to staff at logon to CFPB systems through a warning page. For information not collected directly from individuals, such as information collected during investigations, CFPB provides constructive notice of CFPB's information practices through CFPB's privacy policy, this PIA, and the associated SORNs.

CFPB may use the PII to support litigation or enforcement activities. In these instances, individuals are not given the opportunity to consent to the collection and use of their information, as doing so may interfere with the litigation or enforcement activities.

Wherever required, CFPB also provides notice to individuals about how their information is shared. In some cases, such as when information is collected pursuant to discovery or a related court order, individuals may not receive notice as to how information will be used or disclosed. In these cases, the use and disclosure of information is controlled by applicable federal law, discovery rules, and court orders. In cases where notice cannot be provided or is not required, CFPB provides constructive notice of how it shares information stored by LTST in SORNs, through this PIA, and through CFPB's privacy policy.

Individuals that provide CFPB with information on a voluntary basis may choose to decline to provide such information (e.g., consumer complaints, voluntary disclosures, whistleblowers). However, individuals do not have a right to decline to provide information that is required by law such as via compulsory process, or in cases where information is gathered from public sources as part of the investigatory process. Moreover, individuals generally do not have a right to consent to uses, including dissemination of the information stored in the system. Additionally, a large portion of the data collected in the system is provided by financial institutions pursuant to applicable laws and regulations, rather than directly from individuals, or through investigatory means which may include the collection of publicly available information.

Third-party individuals who may be named within investigations, enforcement, or litigation activities do not have the ability to consent to the use of their information or to obtain redress, as providing consent and redress may interfere with the litigation or investigative proceedings.

CFPB gives individuals the ability to request access and amendment to their personal information in accordance with the Privacy Act and CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq, except where such information is exempt from disclosure as described therein. Information about Privacy Act requests are available at www.consumerfinance.gov/foia. Such exempt material, which is law enforcement-sensitive, may not be able to be accessed or changed, pursuant to 12 CFR 1070.60 and 5 U.S.C. § 552a(k)(2).[5]

5. Explain the standards and relevant controls that govern CFPB's—or any third-party contractor(s) acting on behalf of

[5] Please see the corresponding SORNs for published exemptions under the Privacy Act.

CFPB—collection, use, disclosure, retention, or disposal of information.

A full security review of LTST has been conducted by CFPB based on all applicable federal laws, directives, and standards. CFPB has developed and followed a Security Implementation Plan (SIP) identifying the necessary steps to store PII. Additionally, all systems and applications within LTST are subject to and follow the CFPB risk management processes prior to their uses.

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

- Audit logs and reviews are in place to identify, review, and assess unauthorized access to the LTST environment and the data within its applications;
- CFPB's general privacy training and role-based privacy training are required prior to granting access to the LTST environment and any applications within the platform. Role-based training includes data handling procedures, incident and breach response procedures, and CFPB's authority to collect and use information in accordance with its regulations;
- CFPB's incident response procedures and privacy breach response procedures are in place to address incidents involving data residing in the LTST environment;
- Compliance with CFPB's cybersecurity policy and procedures is documented within security and privacy implementation plans;
- Data quality and integrity checks are performed in accordance with CFPB's Data Access Policy for any systems using data within the environment;
- Extract logging and 90-day reviews;
- Policy and Standard Operating Procedures;
- Role-based Access Controls: CFPB is responsible for assigning and maintaining roles and permissions within LTST and its applications based on an individual's role within the organization and as approved by CFPB Cybersecurity. LTST oversees the portfolio of applications and tools and works with program managers to develop, manage, and provide access to the tools based upon a need to know. No role has full access to all LTST applications. Each role has access to files that are loaded into a workspace in which they have a need to know. The following individuals have access to the system:

- Attorneys
- Paralegals
- Legal counsel
- Case managers
- Contractors
- System administrators
- Developers (support-basis only)
- FOIA analysts
- Resume reviewers
- Comment reviewers.

- LTST hosts and provides end-user support for a suite of applications, systems, and processes to manage these legal activities. The applications and systems that are used to manage the legal activities are as follows; Nexidia, Relativity, IPRO eCapture, Compliance tool, FDMS, ENForce, and FOIAXpress. The National Archives and Administration (NARA) General Records Schedules and NARA-approved Bureau record schedules that are relevant to the information and support are as follows:
  - CFPB N1-587-12-8 (Item 8)
  - CFPB N1-587-12-13 (Item 2c)
  - General Records Schedule 4.2 – Information Access and Protection Records (Item 1, 20, 40, 50, 140, and 180)
  - General Records Schedule 5.2 – Transitory and Intermediary Records (Item 10 and 20).
- Personnel Security, including background checks, is completed for all CFPB employees, contractors, or other individuals authorized to conduct CFPB activities within LTST.

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 safeguards. Other requirements placed on contractors may include training on privacy and compliance with federal privacy requirements and Federal Acquisition Regulations (FAR).

As a result of this PIA, CFPB has identified that cloud-based and desktop tool implementation provides an enhanced security and privacy posture around the sharing of information and tools such as these, will be considered in future enhancements to support investigative proceedings.

6. Discuss the role of third party(ies) that collaborate or partner with 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 CFPB, e.g., government contractors discussed in Question 5.)

CFPB may share PII with external federal and state entities as required and permitted by statute and regulation. CFPB may also share PII with courts, opposing counsel, defendants, paralegals, expert witness, and other individuals as authorized or required by statute, regulation or court rules. CFPB shares information with these external parties to fulfill its enforcement responsibilities, to defend itself in litigation, or pursuant to statutory or regulatory requirements. LTST provides the capability of sharing and collecting PII based upon the direction of the requesting CFPB program. If information is shared, LTST uses tools such as secure file transfer application or an encrypted thumb drive/CD. Sharing datasets that LTST collects will follow and comply with program and privacy compliance requirements as described within CFPB PIAs and SORNs.

Document control

Approval

CHRISTOPHER CHILBERT
Digitally signed by CHRISTOPHER CHILBERT
Date: 2024.01.02 12:53:21 -05'00'

Chris Chilbert

Chief Information Officer

Date

KATHRYN FONG
Digitally signed by KATHRYN FONG
Date: 2024.01.04 14:29:58 -05'00'

Kathryn Fong

Chief Privacy Officer

Date

PAUL IZZETT
Digitally signed by PAUL IZZETT
Date: 2023.12.22 11:14:35 -05'00'

Paul Izzet

Program Lead

Date

Change control

Version	Summary of material changes	Pages affected	Date of change
v.2	Updated PIA to include new tools and technologies.	All	12/2023