Salesforce Platform (Cloud Environment) v.2

Privacy Impact Assessment

August 04, 2025

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law No. 111-203, Title X, 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 executing its duties, the CFPB performs several consumer and stakeholder relationship management and internal employee collaboration activities through a variety of business processes that are supported by information technology (IT) systems and applications. The CFPB uses Salesforce, Inc. (Salesforce) cloud services to modernize its IT portfolio, to increase the efficiency and effectiveness of its consumer service management business processes, and to decrease the cost of hardware and software required by traditional systems and applications to support those business processes.

Salesforce is an external, Platform as a Service (PaaS) cloud-based customer relationship management platform offering extensive options for configuring workflows, databases, forms, dashboards and reports, process modeling, and customizable user interfaces. Salesforce provides a selection of 'out of the box' functionality and custom tools to build internal and external facing applications that support various efforts such as consumer engagement and outreach, relationship management processes, employee collaboration, and internal workflows. Salesforce enables the CFPB to quickly and efficiently build secure applications that automate manual business processes. These processes may involve the collection of personally identifiable information (PII) from consumers or other members of the public, external partners and stakeholders, and CFPB Staff. The type and scope of PII collected varies depending on the CFPB use case.

The CFPB's use of Salesforce is authorized by Sections 1011, 1012, and 1021 of the Dodd-Frank Act. In addition, specific CFPB programs use and collect PII through Salesforce in accordance with legal authorities under which the programs operate. Information in Salesforce is collected in accordance with and is compliant with the Paperwork Reduction Act, the Right to Financial Privacy Act, and the Privacy Act of 1974. The use of Salesforce as a third-party cloud environment is also subject to the terms and conditions set forth in CFPB's contract with Salesforce as the vendor, to include the provisioning of the environment, service level agreements for the ongoing maintenance of the environment, and licenses provided to the CFPB for use of the environment.

Salesforce manages CFPB's technical cloud infrastructure on behalf of the CFPB, including general cloud environment tools such as data storage, system computing resources (such as routers and firewalls, data centers), software maintenance (such as security patches and secure upgrades

to the environment), and access management tools. Salesforce provides access to its environment tools and services to CFPB to build systems and applications to facilitate customer service and business processes, including:

- The collection and use of data via phone, web forms, chats, and email, allowing the CFPB to quickly address consumer cases or complaints.
- Integrated, prebuilt case management tools and capabilities allowing the CFPB to handle case management activities, such as scheduling of meetings and interviews.
- The ability to integrate data held within transitional data systems and databases, saving the CFPB time and resources otherwise spent on data migration activities.
- The ability to build applications that the CFPB uses to automate Helpdesk ticket resolution, escalate consumer concerns and complaints, and address consumer issues and concerns.
- Standardized data collection methods and processes, such as standardizing the format of mailing addresses and customization of form fields, to collect the same type and amount of data to reduce duplicative and incorrect information.
- AppExchange, the suite of CFPB authorized internal and third-party tools offered within the environment to support system development, administration, maintenance, and data storage.

CFPB Salesforce data is hosted and stored in the Salesforce Government Cloud, which is a Compliant Cloud System with Agency Federal Risk and Authorization Management Program (FedRAMP) High Authorization. Salesforce also integrates with other CFPB-authorized third-party cloud system environments for purposes such as the storage of data. The integration allows data within Salesforce to be archived and stored securely within other CFPB-authorized cloud environments to reduce the cost of data storage, scan data and documentation to determine threats such as viruses prior to upload, and system security logging and monitoring tools to ensure authorized access to the environment. All third-party cloud systems that connect with Salesforce are assessed according CFPB's assessment and authorization (A&A) processes to ensure risks are identified and mitigated prior to use.

Authorized CFPB program managers, business product and system owners, system developers and business analysts, and other internal CFPB stakeholders and users, can access Salesforce to leverage these technical capabilities to build systems and applications in a secure, consistent method. Salesforce, and applications developed within Salesforce, are managed through the CFPB Enterprise Platforms Salesforce Center of Excellence (COE), CFPB Change Control Board (CCB) processes and A&A documentation, and addresses privacy relative to systems development to

include functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and privacy risk assessments.

The CFPB initially published this privacy impact assessment (PIA) in April 2022 and is updating the PIA to reassess its use of Salesforce and document the privacy protections that are in place for the PII collected, used, shared, and maintained by the CFPB. This PIA also covers the use of the Salesforce Own solution that is used to archive, backup, and restore Salesforce data. The scope of this PIA is limited to the privacy risks and technical controls associated with the maintenance and use of data within the Salesforce platform. The information of Bureau personnel that is collected for authentication purposes is covered under CFPB.014 Direct Registration and User Management System (DRUMS) System of Records Notice (SORN). Specific use cases and applications developed within Salesforce, and the analysis of the collection and use of PII, are assessed and documented within application specific PIAs[1]. The CFPB's authority to collect specific information, and routine uses of those records, are identified in the associated SORN[2]. Program specific uses of data that require Paperwork Reduction Act approval are also documented within the corresponding application specific PIAs.

Privacy Analysis and Risk Management

The CFPB conducts PIAs on both programs and information technology systems, pursuant to the E-Government Act of 2002, Section 208[3] and in alignment with Office of Management and Budget[4] (OMB) guidance and the National Institute of Standards and Technology (NIST) standards. This PIA examines privacy risks and describes mitigation measures associated with the Salesforce Platform Cloud pursuant to the Fair Information Practice Principles. This includes the

[1] Application specific PIAs that address the maintenance and use of data within the Salesforce environment are found at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

[2] Please see https://www.consumerfinance.gov/privacy/system-records-notices/ for a list of SORNs.

[3] 44 U.S.C. § 3501 note.

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

design and implementation of administrative, technical, or physical safeguards or controls, as applicable.

1. Characterization of Information

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

The PII collected within Salesforce varies depending on the specific application use case; however, the information may include first name, last name, associated entity, phone number, email address, mailing address, military information (including branch, rank, location, service status), employer, position/title, employer's address, place of birth, date of birth, sex, and race/ethnicity. The PII collected and used within Salesforce applications may include:

- Collection, use, and storage of PII within documents related to CFPB's examination and supervision operational and administrative processes.
- Creation, management, and reporting of case records and legal matters that are managed by automated workflows created with Salesforce to allow faster analysis and decision making by the CFPB.
- Collection, administration, and management of the consumer complaint process.
- Tracking, analysis, and management of internal and external correspondence to include automated scheduling and tracking of responses to inquiries.
- Creating, sending, and tracking emails and/or texts to external stakeholders.
- Increased ability to perform trend, pattern, and correlation analysis of large data sets to provide faster consumer response, examination, and supervision processes.
- Collecting, organizing, sanitizing, and sharing data for public consumption.

Although the Salesforce Platform itself does not collect any PII (information is collected through custom applications and forms), it does process PII for authentication purposes. The Platform is connected to Entra ID for internal CFPB users, which uses name and email address to authenticate and provision access. Authorized external users must log in to the applications using an email, password, and multi-factor authentication.

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

The CFPB uses its Salesforce applications to support a wide variety of CFPB activities. Such activities may involve collecting and maintaining PII and other related data of CFPB Staff (e.g., employees, contractors, interns, and, detailees); individuals involved in supervisory, enforcement, or other legal matters with the CFPB, including CFPB employees and external individuals such as judges, opposing counsel, expert witnesses, arbitrators, and mediators; confidential information (CI) or other data about financial institutions; members of the public, including consumers who submit a complaint or inquiry to the CFPB, or who have subscribed to receive general information; and other related routine business communications and data such as day-to-day email communications and work documents to support business functions.

The CFPB can collect data from individuals through the creation of web forms, website submissions, or by submitting data to the CFPB via mail, email, or phone that is then uploaded by Bureau Staff.

The Salesforce Platform is connected to Entra ID to authenticate access for internal CFPB users.

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

The data CFPB collects from individuals through the creation of web forms, website submissions, or by submitting data to the CFPB via mail, email, or phone that goes beyond basic identifying questions must comply with PRA requirements. If required, OMB approval must be obtained through one of CFPB's generic information collection plans or a full clearance package. The appropriate PRA language for these collections is documented within application specific PIAs.

1.4 Discuss how the accuracy of the information is ensured.

The applications created within Salesforce collect information voluntarily, allowing an individual to provide accurate information while providing notice of collecting PII at the time of collection, minimizing the risk of inaccurate data collection. To mitigate these risks the CFPB implemented controls that restrict access to data and changing permissions to restrict changes to information by unauthorized parties, regularly backs up data that can be restored in the event of an unauthorized modification of data, and maintains audit logs to determine when data is added, modified, or deleted.

Privacy Impact Analysis: Related to Characterization of the Information.

Privacy Risk: Since Salesforce provides the ability to create several diverse types of applications with the ability to collect large amounts of information, there is a risk that information collected over time may be inaccurate, outdated, or incomplete.

Mitigation: The applications created within Salesforce collect information voluntarily, allowing an individual to provide accurate information while providing notice of collecting PII at the time of collection, minimizing the risk of inaccurate data collection. Additionally, each application is assessed through ATO processes to ensure that the purpose of each collection is specific to the use within the application.

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 assesses each programs collection of data to ensure the collection falls under a legal authority to do so, and that the PII collected is the minimum amount required to complete program objectives. Salesforce provides environment tools and components that allow the CFPB granular control of data collection options, such as the customization of data fields to limit the amount of PII entered by individuals. How data is collected, the sources of those collections, and how data is minimized to the amount necessary are identified in application specific PIAs.

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.

Each collection of data at the application level has a records schedule that has been submitted to and approved by National Archives and Records Administration (NARA). The deployment of the Salesforce Own solution enables CFPB to archive Salesforce data that needs to be maintained in accordance with its retention schedule. Applications that collect, use, maintain, and/or share PII may retain records indefinitely until the NARA approves the CFPB's records disposition schedule. Records that fall under a general records schedule are maintained and disposed of according to the applicable schedule identified within application specific PIAs and the covering SORNs.

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

Privacy Risk: There is a risk that the PII collected may be used in ways that are not necessary for the purpose of collection.

Mitigation: To mitigate this risk, the CFPB reviews collections of data within each application to minimize the collection of PII to the greatest extent possible, while allowing CFPB to complete its objectives. This may be achieved by stripping collections of PII, aggregating data, or other means of minimizing such collection. Nevertheless, the CFPB necessarily collects PII under its legal authorities and consequently utilizes appropriate technical, physical, and administrative controls relative to the risk of the data within Salesforce. Salesforce provides development tools and components that allow granular control of data collection options, such as the customization of data fields to limit the amount of PII entered by individuals to the minimum amount necessary. These controls are discussed below and in the appropriate PIA and SORN associated with a specific collection of PII.

Privacy Risk: There is a risk that the information collected may be maintained for longer than necessary whereby increasing the risk of exposure and unauthorized access.

Mitigation: This risk is mitigated through the use of Salesforce Own for data archiving certain data. Own is a cloud data protection platform designed to manage and protect mission-critical data from Salesforce. It allows the CFPB to remove inactive data from the production environment and store it in a secure, immutable archive in encrypted format in accordance with applicable retention schedules. Own can only be accessed by a limited number of authorized CFPB personnel.

3. Uses of Information

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

Salesforce provides an ability to collect, process, and store PII to support a variety of CFPB programs and business functions through the development of and management of applications within the cloud environment. The CFPB's objectives include but not limited to the following:

- Creating applications or forms to collect and manage feedback, correspondence, or submissions to CFPB, including but not limited to:
    - Consumer complaints or inquiries about financial products, services, and the entities providing them.

- Examinations and monitoring of bank and non-bank entities.
- Whistleblower tips and contact information concerning companies or individuals that may be in potential violation of consumer protection laws.
- Individual submission of credit card agreements and survey details on behalf of an entity for CFPB analysis.

- Providing responses to external entities (e.g., consumer, industry stakeholders) who submit inquiries by email, voicemail, and web form submissions built within Salesforce.
- Providing case management capabilities to better track litigation and non-litigation cases management by CFPB's Legal Division and tracking that collects PII to facilitate matters.
- Providing a consolidated database to make inquiry management processes more efficient and providing more ways to collaborate and have insight into the Bureau's overall inquiry management and response process.
- Providing applications to track and manage divisional and office budget and procurement actions.
- Data archiving that allows users to store inactive data in a secure environment.

When a program proposes a specific collection of data, the CFPB assesses the design and purpose of the system, to include a collection of PII, through system design documentation reviews to verify the CFPB has an authorized purpose to collect and use the information. Each programs use of PII is also assessed to determine the impact to privacy, and resulting risks are documented within application specific PIAs. Specific collections and methods of collection are further described in application specific PIAs.

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

The Salesforce Platform only stores the data for each Salesforce application, and the data within the applications is separately accessed by the application user with a need to know. Any sharing by a Salesforce application is detailed in the application specific PIA.

Privacy Impact Analysis: Related to Uses of Information

Privacy Risk: There is a risk that the CFPB may use data beyond the intended purpose of collection, and that disparate data sources may be combined and used in new ways that are not consistent with the initial collection.

Mitigation: The CFPB mitigates this risk by conducting program and application specific PIAs to assess the collection and uses of PII in accordance with the authority to collect PII. The CFPB addresses privacy implications during the development lifecycle of an application to ensure that this privacy risk is managed throughout the development lifecycle, and continuous monitoring on systems and applications to ensure the purpose of collection remains consistent.

Privacy Risk: There is a risk that data stored within another cloud environment may be accessed by an unauthorized individual or that a breach within the cloud environment may impact business operations within Salesforce.

Mitigation: The CFPB mitigates this risk by sharing Salesforce data only with systems that have achieved an Authority to Operate (ATO) based upon the CFPB assessment & authorization (A&A) processes. Connections between other cloud environments is assessed by the CFPB to apply role-based environment access controls to ensure the security and privacy of the interconnection. Any proposed data sharing between the cloud environments is also assessed to ensure only authorized individuals can access data within Salesforce.

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.

The CFPB provides notice on how the CFPB collects and uses PII through the publication of this PIA, associated SORNs, and Privacy Act statements and notices, as applicable. When practicable and/or required by law, the CFPB provides notice of the uses of PII and the opportunity to consent to uses at the time of collection. These notices are located on Salesforce application-hosted webpages, web forms, electronic collections, and on forms used by individuals to submit information to a Salesforce application.

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 applications created within Salesforce collect information voluntarily, and individuals receive notice via Privacy Act statements and privacy notices, as applicable, provided at the point of collection. This provides the individual the opportunity to consent to uses of their information at the time of collection. While individuals can choose not to provide their information, doing so may limit the CFPB's ability to perform the requested service.

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

CFPB provides individuals the ability to request access and amendment to their PII in accordance with the Privacy Act and 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. Individuals may sometimes be able to directly update their information – for example, by contacting the CFPB directly to update contact or mailing information, or updating information provided for registration purposes for a CFPB-sponsored event.

Privacy Impact Analysis: Related to Individual Notice and Participation

Privacy Risk: There is a risk that individuals do not understand the functionality of Salesforce and how their data is used by applications within the environment.

Mitigation: Salesforce provides a suite of standardized tools and components that are native to the Salesforce environment. CFPB uses these tools to develop several applications within the environment, each with a specific collection and use of data, to include PII. The CFPB mitigates this risk through Privacy Notices, Privacy Act Statements, PIAs and SORNs to help individuals understand the purpose of Salesforce and describe how their PII is collected, used, shared, and maintained within the environment. Included within these documents are ways in which individuals can contact the CFPB to learn about how PII is used within specific applications in Salesforce.

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 Salesforce Platform does not share information externally. Individual Salesforce applications may share with external entities on a need to know basis. The entities with whom applications may share information are identified in application specific PIAs that can be found on the CFPB's website located at https://www.consumerfinance.gov/privacy/privacy-impact-assessments/.

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

The Salesforce Platform does not share information externally. Individual Salesforce applications may share with external entities in accordance with the routine uses identified in the applicable SORN. The limitations on information sharing are identified in application specific PIAs that can be found on the CFPB's website. Typical controls include memoranda of understanding, information sharing agreements, and authority to use. These controls describe the information that may be shared with the entity and any limitations placed on the external entity regarding further sharing. Furthermore, external entities must have a Salesforce account through which the CFPB shares information. This ensures that any information shared is transmitted to the correct person with a need to know.

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

Privacy Risk: There is a risk that information residing on the Salesforce Platform may be inappropriately shared externally.

Mitigation: To mitigate this risk, the CFPB has implemented administrative and technical access controls that help to ensure information maintained within the applications is used and shared according to the purposes identified in this PIA and other related notices. Only CFPB Staff have direct access to all the information collected and maintained in the applications. Further, CFPB customizes Salesforce capabilities to limit the use and access to data in accordance with CFPB policies.

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,[5] the Right to Financial Privacy Act,[6] and the E-Government Act of 2002, Section 208.[7] To ensure compliance, and that PII and other sensitive information is protected, the CFPB adopted the Fair Information Practice Principles (FIPPs) as the

[5] 5 U.S.C. § 552a.

[6] 12 U.S.C. § 3401 *et seq.*

[7] 44 U.S.C. 3501 note.

framework for its privacy policy.[8] The FIPPs apply throughout the CFPB for the collection, use, maintenance, disclosure, and destruction of PII, and any other activity that impacts the privacy of individuals, regardless of citizenship, to ensure compliance with all laws, regulations, and policy requirements.

The CFPB adheres to the Office of Management and Budget (OMB) privacy-related guidance and applies the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) for information technology systems, applications, solutions, and services.[9] 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.[10] The Authority to Operate was completed for the Salesforce platform.

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 shortly after their onboarding 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. Some Salesforce application users have an additional role-based training to understand the privacy responsibilities related to their specific roles.

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

---

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

[9] *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.

[10] *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.

CFPB Staff with access to CFPB information, 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). This ensures the CFPB maintains a secure operating environment and protects our systems against potential external threats.

In addition, the CFPB employs role-based access controls. The CFPB uses role-based access controls to ensure users only have access to the system and/or information necessary and relevant to their assigned duties. Individuals who no longer require access have their credential removed from the system. All roles are documented within the Salesforce AMP, and Entra ID is utilized to log in to Salesforce through the SAML 2.0 Single Sign On (SSO) process. Regular accounts are automatically provisioned through the identity management solution, SailPoint.

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

Privacy Risk: There is a risk that unauthorized users may access the Salesforce Platform or be granted access to Salesforce applications.

Mitigation: CFPB information is hosted on a dedicated Salesforce Government Cloud Plus environment, that has been built on an AWS GovCloud instance. Salesforce Government Cloud Plus is a Compliant Cloud System with FedRAMP High Authorization. Information within Salesforce is therefore subject to the appropriate technical, physical, and administrative controls implemented through the CFPB's National Institute of Standards and Technology (NIST) based risk management process that identifies risk, analyzes the risk, prioritizes the risk, and develops plan to remediate the risk.

It is through these processes that controls such as encryption for data maintained within the system are implemented to reduce overall risk to the data within the system. Security and privacy controls are implemented within the Salesforce environment and are also implemented within systems and applications built within the environment to restrict access to the information to authorized

individuals. Access controls supported by role-based privacy training for individuals who handles data further helps to mitigate this risk. Application specific PIAs are also completed for all applications within Salesforce that collect, use, share, and maintain data to identify roles for accessing data. Additionally, both internal and independent auditors hold the CFPB accountable for complying with CFPB policies and procedures related to the processing of PII. The CFPB is committed to taking swift and immediate action if there are any violations of law, policies, and procedures.

In addition to the above technical, physical, and administrative controls to safeguard PII and other sensitive information maintained on the Platform, 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.

Document control

Approval

_____

Christopher Chilbert

Chief Information Officer

Date

_____

Kathryn Fong

Chief Privacy Officer

Date

_____

Danny Pham

Program Owner

Date

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

Change Control

Version	Summary of material changes	Pages affected	Date of change
1.0	Initial publication	All	April 2022
2.0	General updates to controls and to document Salesforce Own	All	August 2025