PRIVACY IMPACT ASSESSMENT— AUGUST 2024

Consumer Response System v.2

Does the CFPB use the information to benefit or make a determination about an individual?	No.
What is the purpose?	Manage the collection and response to consumer complaints.
Are there controls to enforce accountability?	Yes, all standard CFPB privacy protections and security controls apply.
What opportunities do I have for participation?	Appropriate opportunities for notice, consent, access, and redress.

Consumer Financial Protection Bureau

Overview

The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "Act"), Public Law No. 111-203, Title X, established the Consumer Financial Protection Bureau (CFPB). The CFPB implements and enforces Federal consumer financial law and ensures that markets for consumer financial products are fair, transparent, and competitive. The Act establishes collecting, investigating, and responding to consumer complaints as one of the CFPB's primary functions.[1] The Act also requires the CFPB to establish a unit responsible for the centralized collection of, monitoring of, and response to consumer complaints about consumer financial products or services,[2] establishing reasonable procedures to provide timely responses to consumers regarding their complaints,[3] and sharing consumer complaint information with prudential regulators, the Federal Trade Commission (FTC), other Federal agencies, and State agencies.[4]

To fulfill these requirements, the CFPB established the Office of Consumer Response (Consumer Response). Consumer Response maintains procedures to provide a timely response to consumers,[5] in writing, to complaints[6] concerning a covered person.[7] Consumer Response also created and manages the Consumer Response System (CRS).[8] The CRS is a case management system that operates on the CFPB's Salesforce environment, a vendor-provided service and

---

[1] *See* 12 U.S.C. 5511(c)(2).

[2] *See* 12 U.S.C. 5493(b)(3).

[3] *See* 12 U.S.C. 5534.

[4] *See* 12 U.S.C. 5493(b)(3)(D).

[5] *See* 12 U.S.C. 5481(4).

[6] Consumer complaints are submissions that express dissatisfaction with, or communicate suspicion of wrongful conduct by, an identifiable entity related to a consumer's personal experience with a financial product or service. *See* Consumer Financial Protection Bureau, Consumer Response Annual Report (Mar. 2012), available at http://files.consumerfinance.gov/f/201204_cfpb_ConsumerResponseAnnualReport.pdf .

[7] *See* 12 U.S.C. 5481(6); 12 U.S.C. 5534(a).

[8] *See* The Dodd-Frank Wall Street Reform and Consumer Protection Act ("Act"), Public Law No. 111203, Title X grants the CFPB authority to operate the CRS. Specifically, Pub. L. No. 111-203, Title X, Sections 1011, 1012, 1013(b)(3), 1021, 1034 codified at 12 U.S.C. §§ 5491, 5492, 5493(b)(3), 5511, 5534.

cloud platform.[9] The CRS provides an online web portal through the CFPB website (i.e., the Consumer Portal) where consumers create an account to submit a complaint to the CFPB. The CRS also includes complaints submitted by telephone, postal mail, and referral. Through the CRS, Consumer Response accesses, inputs, manages, and responds to consumer complaints. Additionally, the CRS establishes separate portals for authorized external users to access consumer complaints. This includes users of the Company Portal (i.e., users from identified companies or entities that the complaint may be about), Government Portal (i.e., users from federal, state, or local agencies), and Congressional Portal (i.e., users from Congressional offices) (herein collectively referred to as portal users).[10] The CRS collects and uses personally identifiable information (PII) of consumers and portal users who create a secure online account within the CRS in order to submit, view, and/or manage a complaint. Additionally, consumers may provide PII in the complaint itself, which is also maintained within the CRS.

In addition to facilitating the consumer complaint process, Consumer Response maintains a suite of analytics tools called Complaint Explorer.[11] This toolkit provides users the ability to search, filter, and visualize complaint information, to compile data reports, and to examine trends and information about the consumer complaint landscape using data from the CRS. Complaint Explorer was previously an internal CFPB tool only accessible to CFPB users; however, Consumer Response is expanding its use to provide access to authorized external federal, state, and local government agencies with executed Government Portal Agreements through their existing access to the Government Portal.

The CFPB is conducting this Privacy Impact Assessment (PIA) to assess the privacy risks associated with the collection and use of PII within the CFPB's CRS. The CFPB is updating the Consumer Response PIA that was previously published in March 2013 to reflect the enhancement to the Complaint Explorer analytic toolset within the CRS, as well as to document

---

[9] For more information, see the Salesforce Platform (Cloud Environment) PIA on the CFPB website: www.consumerfinance.gov/privacy/privacy-impact-assessments.

[10] For this PIA, the term "portal users" refers to all users of the Company Portal, Government Portal, and Congressional Portal collectively when there are technical design or security similarities between all three portals. When there are differences among the three portals, distinctions are specified. The term does not refer to Consumer Portal users who are referred to as "consumers" throughout this PIA.

[11] Complaint Explorer is hosted within CFPB's Amazon Web Services cloud environment. For more information, see the CFPB Alto General Support Services PIA located at www.consumerfinance.gov/privacy/privacy-impact-assessments.

current processes and functionality related to the CRS, described below. Consumer complaints received and maintained by the CFPB are subject to the System of Records Notice (SORN) CFPB.005—Consumer Response System.[12] Pursuant to the Paperwork Reduction Act, the CFPB has received OMB approval under control number 3170-0011 for collections associated with the CRS.

Submission of Consumer Complaints, Inquiries, or Feedback

All portal users, as well as consumers, must have accounts within the CRS in order to log in to their respective portals. To create an account, all users must provide limited PII, including name and contact information, and then create a password to access the account.

The CRS collects consumer PII in various ways: 1) when a consumer directly submits a complaint through the web portal; 2) when a consumer calls the CFPB's toll-free number or mails information to the CFPB; 3) when a consumer complaint is referred to the CFPB on behalf of a consumer by a third party such as a Congressional office or government agency; or 4) when consumers choose to submit an inquiry about their experiences with financial products or services.[13]

Once the consumer creates an account, they are able to submit a complaint directly through the web portal. The consumer is then prompted to submit the PII necessary for their specific complaint based on the financial product or service that pertains to their complaint. In addition to name and contact information and some selectable options associated with a complaint, such as financial product or service type, the form prompts the consumer to provide a narrative description of their issue and the proposed resolution in free-form text boxes. The form instructs the consumer to not provide PII in their narrative description; however, a consumer may provide PII in their narrative while providing details that they believe are relevant to their complaint. The form also provides an option for the consumer to upload documentation to support their complaint. The documentation that a consumer chooses to upload may contain PII such as their name, contact information, and financial account numbers. The complaint form contains additional fields where the consumer has the option to provide specific PII such as an

[12] For all CFPB SORNs, please visit: www.consumerfinance.gov/privacy/system-records-notices.

[13] Consumer Response discontinued accepting complaints by fax in May 2021 due, in part, to declining use of this submission channel by consumers.

account or loan number to help the company identify the consumer in their system. The consumer also can optionally provide demographic information to be associated with their complaint, such as age or race.

Consumers can alternatively choose to submit complaints or make an inquiry by calling the CFPB's toll-free number or submitting information to the CFPB's mailing address. The Consumer Resource Center (CRC) is responsible for responding to consumers' calls and processing mail submissions.[14] Mail submissions are scanned and manually entered into the CRS by a Consumer Guide[15] at the CRC. For complaints, the CRC enters in the CRS the same PII over the phone or through scanned mail as consumers would provide online. The CRC creates an account or matches a consumer to an existing account using name and contact information, when possible. This PII, along with complaint details and supporting documentation, is used to create and process the complaint. For more information regarding the CRC and intake processes, see the Consumer Resource Center (CRC) PIA.[16]

The CFPB may also receive a consumer complaint through a third-party referral such as from a Congressional office, the White House Executive Office, or other agencies (e.g., the Office of the Comptroller of the Currency). In some instances, a CRC Consumer Guide enters the consumer's name and contact information into the CRS to create an account for the consumer or match to an existing account. This PII, along with complaint details and supporting documentation, is used to create and process the complaint.

In addition to submitting complaints, consumers can choose to share their experiences regarding financial products or services in a "Tell Your Story" narrative submission through the website consumerfinance.gov/your-story/ or by phone. Consumers have the option to provide limited PII, such as name and contact information, but are not required to do so. Consumers can

---

[14] Consumer Response, with vendor assistance, operates the CRC, to directly interact with consumers for the intake of complaints and to field inquiries.

[15] Consumer Guides are representatives of the CRC that are contracted by the CFPB to intake and process complaint submissions that are submitted through the phone, by mail, and through referrals. They also answer questions and provide complaint status updates after verifying the consumers through name and contact information associated with the complaint.

[16] For more information see the Consumer Resource Center (CRC) PIA on the CFPB website: www.consumerfinance.gov/privacy/privacy-impact-assessments.

also grant the CFPB permission to share their experiences with the public and with external stakeholders. Unlike consumer complaints, submission of these "Tell Your Story" narratives does not require that the consumer create an account in the CRS. These submissions are not published in the public Consumer Complaint Database,[17] sent to companies for a response, or shared via the Government Portal.

Disclosure to an External Company

When a consumer submits a complaint about a company, Consumer Response routes the complaint—and any documents the consumer provides, including PII—directly to the company for response. The transmission to the company is made through the secure web-based Company Portal. Company users log into the Company Portal to view and respond to complaints sent to their company. A company's response to a consumer's complaint is shared with the consumer via their secure Consumer Portal. Consumers can log in to view the company's response and company response data is stored within the CRS. Consumers are also given the option to provide feedback about the company's response to their complaint. Companies may also send administrative responses to the CFPB when further review may be needed. Administrative responses are stored within the CRS for Consumer Response action and documentation; however, limited information is made available to consumers in the Consumer Portal, and complaints receiving appropriate administrative responses are not published in the Consumer Complaint Database on the CFPB's website.

Disclosure to Federal, State, and Local Government Agencies with Relevant Legal Authorities

Consumer Response shares consumer complaint information—including the associated PII—with agencies that have supervision, enforcement, and/or market monitoring authorities related to depository and/or non-depository providers of consumer financial products and services using a secure Government Portal. For example, the state or federal prudential regulators can use the Government Portal to access complaints where the CFPB and the regulator share supervisory authority. Complaint data is shared with government partners through the Government Portal, which is integrated with Complaint Explorer.

---

[17] The CFPB publishes de-identified complaint information in its public Consumer Complaint Database. Information about the Consumer Complaint Database is available at www.consumerfinance.gov/data-research/consumer-complaints.

Other Disclosures

Consumer Response may share consumer complaint information in several other ways, as follows:

- **Responses to complaint referrals from government agencies:** If the complaint was referred by a government agency, Consumer Response may share the company's response with the government agency.
- **Responses to complaint referrals from Congressional offices:** If the complaint was referred by a Congressional office with a signed privacy release, Consumer Response may share the company's response with the referring office.
- **Responses to complaint referrals from the White House:** If the complaint was referred by the White House, Consumer Response may share the status of the complaint with the White House.
- **Parties in litigation:** Consumer Response may share consumer complaint information with a court, a party in litigation, a magistrate, an adjudicative body, or administrative tribunal in the course of a proceeding, or the Department of Justice.
- **Oversight agencies and law enforcement:** Consumer Response may also share consumer complaint information with oversight agencies such as the Office of Inspector General and the Government Accountability Office or in response to a lawful subpoena or request. PII would only be included where permitted by statute or regulation.
- **Public Disclosure:** Consumer Response makes certain de-identified consumer complaint data available to the public on its website via the Consumer Complaint Database.[18] This can at times include an individual consumer's narrative description of issues raised in their complaint. A narrative is only published if the consumer opts to share it publicly and after Consumer Response takes steps to remove personal information.[19]

Complaint Explorer

[18] The Consumer Complaint Database is available at www.consumerfinance.gov/data-research/consumer-complaints.

[19] For more information, see the Publication of Consumer Response Complaint Narratives PIA on the CFPB website: www.consumerfinance.gov/privacy/privacy-impact-assessments.

Authorized internal CFPB and external Government Portal users can access the Complaint Explorer toolkit to search, filter, and analyze complaints; read consumer narratives and company responses; and display complaints by topic, products, issue, company, geography, and consumer demographics to uncover patterns and view trends in complaint volumes over time. Complaint Explorer also provides users with the ability to download individual complaints and attachments, and export complaint information for authorized purposes such as to support agency supervision, enforcement, and litigation. The data from complaints helps the CFPB and government partners coordinate analyses and improve understanding of the financial marketplace and consumer concerns.

Privacy Risk Analysis

The following risk categories apply generally across the CRS:

- Security
- Awareness and Training
- Accountability and Auditing
- Data Minimization
- Limits on Uses and Sharing of Information
- Data Quality and Integrity

Security

The CRS stores PII and other sensitive information provided by consumers, including information from third parties submitting complaints on behalf of consumers, and by companies making it a potential target for hackers, identity thieves, and other cyber-threats. The CFPB mitigates this risk by implementing appropriate security controls and safeguards for the CRS to protect the information contained in the system against unauthorized disclosure and access. For example, the CFPB only grants access to the system to authorized users and the level of access provided is based on their need to know.

Authorized users are restricted to the minimum amount of data required to carry out their assigned job responsibilities. For instance, users of the Company and Congressional portals can only access complaints that are related to their specific company or Congressional office, respectively. The CFPB terminates or reduces access once a CFPB employee or contractor no

longer has a need to know the information for their job duties, resigns, or is terminated. Similarly, Congressional-, Government-, and Company-Portal authorized Points of Contact (POCs) are responsible for managing users' access at their respective organization. For Government Portal and Company Portal access to the CRS, the CFPB requests and expects user re-certification to be conducted annually through the portals.

The CFPB Security Operations Center (SOC) monitors daily use of the system for suspicious or possibly inappropriate activity. The CFPB has developed an incident reporting plan and procedures for handling security incidents, including those involving the CRS. The SOC is responsible for reporting any incidents it detects through monitoring and coordinating escalation, reporting, and response procedures on behalf of the CFPB. The CFPB also maintains a privacy breach response plan to handle breaches involving PII, including breaches that involve the CRS. All users that work with the CRS are trained to report suspected security incidents and breaches of PII to the CFPB SOC and Privacy Office for appropriate mitigation.

Additionally, the system owner has and maintains its Authority to Operate (ATO) to continue operations, consistent with federal requirements and National Institute of Standards and Technology (NIST) guidance. The CRS conforms to CFPB security requirements, which was confirmed prior to use.

Awareness and Training

There is risk that CFPB staff or portal users may inadvertently mishandle the PII that is contained in the CRS, which could cause embarrassment and potential financial loss to the consumer, as well as potential loss of reputation, litigation, and financial loss to the CFPB. Such mishandling of PII may include staff or portal users inadvertently providing data to an incorrect recipient, or otherwise allowing unauthorized access. To mitigate this risk, CFPB employees and contractors are required to complete annual privacy training. The CFPB also works closely with the contracted vendor for the CRC to establish and maintain policies, procedures, and administer CFPB privacy and security trainings for individuals who access the CRS. Additionally, Government Portal users receive a CFPB agreement and must attest to the terms to safeguard PII upon each use of the Government Portal and Complaint Explorer. Each time a Government Portal or CFPB user exports copies of complaints, pop-up banners appear to remind them of their responsibility to safeguard PII. The CFPB provides instructions for all CFPB staff, users of Complaint Explorer, and all portal users on how to handle PII and report suspected breaches of PII.

Accountability and Auditing

Due to the sensitivity of the PII contained in the CRS, the many functions it serves, and the number of CFPB staff and portal users who engage with it, regular monitoring is needed to ensure its proper use. The CRS may be a target for malicious users or hackers who intend to do harm to the CFPB or to individual consumers. Without consistent monitoring, PII contained in the CRS could be exposed to unauthorized users or used for unauthorized purposes. To address this risk, the CFPB establishes and maintains policies, procedures, access controls, and auditing capabilities for the CRS, Complaint Explorer, Company Portal, Government Portal, and Congressional Portal. All users are authenticated at log in. Complaint Explorer users must also sign their initials when exporting complaints. When an external user downloads complaints, an audit log is created detailing the download request. CFPB can use this audit log to monitor and investigate unusual download activity for an authorized user.

Additionally, all users of the CRS are frequently informed of their roles and responsibilities to safeguard PII:

- All CFPB and CRC staff receive onboarding and annual privacy awareness training.
- All Complaint Explorer users must attest that they agree with CFPB requirements to safeguard PII each time they access Complaint Explorer.
- When Complaint Explorer users export complaints, they are reminded of responsibilities to minimize the exporting of PII and to safeguard exported complaint information. They must agree to the terms of use for disclosure that specifies the CFPB clearance requirements for authorized disclosure and distribution.
- Privacy guidance is provided in the Complaint Explorer export training module for all users.
- Government Portal authorized representatives certify that their agencies agree to the terms of use for the Government Portal Agreement and attest that all users of the agency will follow the requirements to protect PII.
- In addition to the reminders that all Complaint Explorer users receive, all Government Portal users receive instructions to protect PII each time that they access the Government Portal and agree to the requirements of the Government Portal Agreement.

As mentioned in the Security section, the CFPB performs regular security monitoring to determine if inappropriate access has occurred, this includes maintaining and monitoring audit logs. To prevent and respond to suspected or confirmed unauthorized access or use of the CRS,

the CFPB has put in place incident-reporting and privacy breach response plans and procedures for handling suspected security incidents or breaches.

Data Minimization

Consumer Response has assessed its operations and determined the minimum PII that is required to be collected and used to process consumer complaints, used for internal CFPB analysis, and shared with companies, government agencies, and Congressional offices. However, there is a risk that consumers may submit more PII than necessary when submitting a complaint. For example, an individual could unnecessarily provide their personal financial information, health information, or other types of PII in their complaint description. To mitigate this risk, for complaint submissions received through the website, the online complaint form cautions the submitter not to include PII in their complaint narrative since it will be collected separately in dedicated fields later in the complaint form. Consumer Response designed the online complaint form to streamline the collection of PII to only include the information needed to help companies identify consumers in their own records. For example, effective July 2023, consumers are only given the option to provide the last 4 digits of their Social Security Number (SSN) instead of their full SSN when submitting credit reporting and student loan complaints. This information is often necessary to distinguish consumers in the company's records. Similarly, the same approach promoting minimization is applied to other data fields where possible, such as only collecting account numbers where necessary to help companies respond to complaints.

The "Tell Your Story" online form instructs consumers not to include sensitive or personal information in their story.

Limits on Uses and Sharing of Information

There is a risk that consumer information may be used beyond the approved purposes. Consumer Response mitigates this risk by ensuring that the information collected through the complaint system is only used for authorized purposes such as analyzing, investigating, and monitoring complaints. Consumer Response also ensures that information is only shared with CFPB staff, companies, government agencies, and Congressional offices with approved data access related to their valid need-to-know.

Complaint Explorer features analytical capabilities and the capability to view, export, and print complaints for authorized purposes such as for trend analysis, supervision and enforcement examinations, and litigation. CFPB and Government Portal users have the option to export full

complaints with attachments in PDF or export multiple complaint records in a CSV or JSON file format. There is a risk that exported complaint information could be mishandled, stored without appropriate access restrictions, lost, or otherwise disclosed without authorization. To minimize the risk of a security incident or breach, there are several mitigations included in the system design and process.

Consumer Response restricts bulk downloads to 500 complaint PDF exports at one time in a Zip file and 10,000 complaint record exports to CSV or JSON files at one time. When users export a single complaint or multiple complaints, consumer name and contact information fields are excluded from the export by default. Users must manually select an option to include consumer name and contact information if they have an authorized business need. Users must attest that they agree with CFPB requirements to safeguard PII when they access Complaint Explorer. When users export complaints, they are reminded of their responsibilities to safeguard PII and they must agree to the terms of use for disclosure that specifies the CFPB clearance requirements for authorized disclosure and distribution. A user's need to access Complaint Explorer and the Government Portal is recertified annually.

The Congressional Portal and Company Portal do not provide access to Complaint Explorer and its analytical capabilities. However, users of these portals are still able to view, export, and print complaints available in their portals related to their specific Congressional Office or company. For the Congressional Portal, there are default bulk export limits of 100 complaints per CSV file. Company Portal users have default bulk export limits of about 1,000 complaints per CSV file and up to 10 files per export. All exports and printing are logged for auditing purposes and the CFPB has provided guidance to users on how to safeguard electronic and hardcopies of PII and how to dispose of hardcopies of PII when no longer needed. The CFPB prompts company-authorized POCs to recertify their users annually.

Data Quality and Integrity

There is a risk of inaccurate information being submitted to the CRS. Consumers and third parties submit information by web, by postal mail, or over the telephone. If over the telephone, there is a possibility that the representative did not accurately record the consumer's submission. This is mitigated by the training the CRS staff has received regarding use of the CRS, the fields that guide what information needs to be entered into the CRS, and the review of the information with the caller before closing out the entry. There is also a risk that the consumer provides incorrect information through the web or by mail or telephone. The CFPB mitigates this risk by ensuring the consumer affirms the following statement: "the information

given is true to the best of [their] knowledge." Moreover, if a consumer uses the web or paper complaint form issued by the CFPB, Consumer Response asks the consumer to affirm the same statement via checkbox selection. When providing information through the web, Consumer Response has built-in processes and controls to mitigate issues with accuracy and completeness prior to and following consumer submission of information. For example, consumers must validate their email address before starting to submit a complaint online. Online forms include field-level data validation rules to ensure completion at the time of submission. Finally, the consumer is prompted to review the information provided on the online complaint form for accuracy before submission.

Regardless of the channel of submission, if Consumer Response determines a complaint is incomplete, Consumer Response may contact the consumer to request that they provide additional information. Additionally, the consumer can contact Consumer Response through the CRC to correct or amend records about themselves or can access submissions online through the Consumer Portal to make corrections. The CFPB also provides consumers a means through the Privacy Act to amend or correct a person's records at their request, or a request made on their behalf. Information about Privacy Act requests is available in the SORN, CFPB.005 – Consumer Response System, and through use of a Freedom of Information Act request, described at https://www.consumerfinance.gov/foia-requests/.

Finally, there is a limited risk that Consumer Response staff may manually route a complaint to an incorrect company. However, this risk is mitigated through functionality to automatically remove entity access to complaint information through administrative response functions. Consumer Response also instructs the entity to delete downloaded complaint information if a complaint is incorrectly routed to them.

The technical, physical, and administrative controls implemented to promote individual participation, minimization, and accountability are appropriate.

Privacy Risk Management

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

The following lists PII or other data which may be included in the CRS categorized by account creation, required PII for complaint submission, and supplemental or optional PII that consumers may be asked to submit:

The CRS collects the following PII for Consumer Portal account creation:

- Consumer's first and last name;
- Email address; and
- Telephone number.

Consumer name and contact information collected through account creation is automatically included for each complaint associated with the account.

The CRS collects the following PII for Company, Government, and Congressional Portal account creation:

- User's first and last name;
- Business mailing address;
- Business email address;
- Business phone number;
- Title; and
- Company, agency, or office name.

The CRS collects the following information during complaint submission process:

- Consumer mailing address;
- Product and issue type (e.g., related to mortgages, credit cards, credit reports, student loans, or other product types) and related questions;
- Name of company;
- Description of event(s) resulting in the complaint;
- Description of desired resolution.

The consumer may choose to provide additional PII as part of their complaint submission, including but not limited to:

- Account identifiers for companies to identify consumers in their records to facilitate their responses (e.g., where applicable, account information, credit card information, receipts or transaction details, last four digits of the SSN);

- Optional demographic and biographic information about the consumer, including servicemember status, household size/income, or inmate number; or
- Information about company employees.

The PII is provided directly by consumers through the Consumer Portal web form, by phone when the consumer calls the CRC, or by mail; or received from companies or those making referrals on behalf of the consumer, including from Congress, the White House, or other agencies. Through the CRS, Consumer Response receives and routes complaints to companies through the secure Company Portal or refers them to other regulators as appropriate.

Consumer Response aims to minimize the amount of information received through the online complaint form by providing instructions for the submitter to not to include PII in their complaint narrative; and only requiring a minimal amount of PII, which is collected in dedicated fields in the complaint form. Additionally, when complaints are submitted through the CRC, Consumer Guides are trained to intake only the minimum PII needed for complaint submission.

2. Describe CFPB's objective for the information.

The CRS collects name, email address, and phone number to create authenticated user accounts and address when the consumer submits a complaint. Consumer Response may use this information to communicate or manage the complaint process, depending on the user's role.

Consumer Response also uses consumer name and contact information to verify a consumer if they contact the CRC to receive updates on their complaint and to provide automated status updates to consumers about the progress of their complaint, or to send an alert if any additional action is needed by the consumer.

Consumer Response uses the complaint information, including PII collected through the CRS, to meet the following objectives:

- Receive consumer complaints and route them for response by the company that is the subject of the complaint, or to another regulator;
- Respond to consumer inquiries by providing necessary information or resources;
- Conduct research and analysis through Complaint Explorer. This analytics tool uses data from the CRS and supports analyses and data visualization to understand trends in the consumer experience. This data can also be helpful in establishing the presence of a

harmful practice in the marketplace for consumer financial products and services. Such information may be analyzed to prepare and publish reports and to facilitate supervisory, enforcement, and market monitoring activities of the CFPB;

- Improve Consumer Response customer service and operations (for example, data associated with a phone interaction may be used to evaluate the performance of Consumer Guides);
- Share complaint data with other authorized federal, state, and local partners through the Government Portal to aid in their business practices in accordance with the Act;[20]
- Provide statutorily mandated reports to Congress; and
- Meet CFPB's statutory objective of ensuring that markets for consumer financial products and services are fair, transparent, and competitive.

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.

Consumer Response makes complaint information available to external users through the various user portals as described above. Consumer Response shares consumer complaint information through the Government Portal with other federal, state, and local government agencies that have supervision, enforcement, and/or market monitoring authorities related to depository and/or non-depository providers of consumer financial products and services. This information includes individual complaint data which may include PII. Each government agency with a signed data access agreement receives secure access. Government Portal users can only access the Complaint Explorer through this secure, web-based channel. Complaint Explorer allows users to view and export consumer complaints and use built-in analytical tools related to data received in the CRS. In addition to the Government Portal, Consumer Response also has data feeds and automated programming interfaces (APIs) with government agencies to facilitate complaint referral and data sharing securely and efficiently.

Consumer Response shares limited complaint information with congressional offices through a secure Congressional Portal. Authorized Congressional Portal users can view complaints they

[20] *See* 12 USC 5493(b)(3)(D).

submit on behalf of their constituents, as well as company responses, if they provide consumer-signed privacy releases. The White House Executive Office makes complaints available to Consumer Response via its own secure system, and Consumer Response enters the complaints into the CRS. As complaints are processed, Consumer Response shares limited complaint status information with the White House Executive Office.

Consumer Response shares complaint information through the Company Portal with users authorized by the company that is the subject of the complaint. Authorized company users can only access complaints about their company so that the company can provide a response to consumer complaints. Consumer Response may also provide information to the company directly, as part of its response to a possible breach by the company or other actions. In the event there is a confirmed company-originated privacy breach, Consumer Response will provide notice to the responsible entity so that it can comply with any state or federal laws, such as the Gramm-Leach-Bliley Act.

Any disclosure of records containing PII is in accordance with the routine uses published in CFPB.005 Consumer Response SORN and as legally authorized. Consumer Response makes certain complaints publicly available after taking steps to remove PII from consumer complaint narratives in the Consumer Complaint Database.[21]

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 consumers about how their information is collected and used through the publication of this PIA, the associated CFPB.005 – Consumer Response SORN, and Privacy Act Statements provided during complaint submission. Any time consumers call the CRC, consumers are advised via an automated prompt that their call may be monitored and recorded for quality assurance purposes. Additionally, when a consumer chooses to submit a complaint via telephone, a Consumer Guide reads a verbal Privacy Act Statement notifying the

[21] For more information, see the Publication of Consumer Response Complaint Narratives PIA on the CFPB website: www.consumerfinance.gov/privacy/privacy-impact-assessments.

consumer that the CFPB is collecting their information and provides notice regarding how their information will be used.

Every consumer who submits a complaint on the website is provided an option to consent and opt-in to the publication of their narrative in the Consumer Complaint Database. Consumer Response does not publish a narrative unless the consumer explicitly consents to the publication and only after taking steps to remove PII. Consumers can withdraw consent at any time by calling the CRC. The database generally updates daily; therefore, if consent is withdrawn, the information from the database will typically be removed from the Consumer Complaint Database the next day. However, data already downloaded by the public cannot be recalled. To help a consumer decide if they want their narrative published, there is a "Learn how it works" link on the complaint form. More information is available in the CFPB Publication of Consumer Response Complaint Narrative PIA.

When consumers submit complaints about a consumer financial product or service, they sometimes include information about employees of the company providing the financial product or service. The CRS also sometimes receives information about company employees through company responses to complaints. The scrubbing process takes steps to remove information that can be used to identify employees of companies prior to publication of the complaint narrative.

Consumers may access their complaint information through the Consumer Portal or can contact Consumer Response through the CRC to access information regarding the status of their complaints and update certain information about themselves (e.g., address). The CFPB gives consumers the ability to request access and amendment to their personal information in accordance with the Privacy Act and the CFPB's Privacy Act regulations, at 12 C.F.R. 1070.50 et seq. Information about Privacy Act requests is available in the SORN, CFPB.005 – Consumer Response System, and at https://www.consumerfinance.gov/foia-requests/.

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 manages risks to privacy by complying with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002. The CFPB voluntarily adopts Office of

Management and Budget privacy-related guidance as a best practice[22] and applies NIST risk management processes for privacy.

The CFPB generally uses the following technical and administrative controls to secure the data contained in the system against unauthorized disclosure and create accountability for the CFPB's appropriate collection, use, disclosure, and retention of the information:

- Personnel Security including background checks;
- Mandatory CFPB information security awareness training;
- Mandatory CFPB privacy awareness training;
- Audit logs and reviews;
- CFPB Privacy Breach Response and Recovery Plan;
- Compliance with CFPB Cybersecurity Policies and Procedures;
- Data quality and integrity checks;
- Extract logging;
- Procedures and guidance;
- Role-Based Access Controls (e.g., the *System Owner* acts as the account manager for all accounts in the system; *Information System Security Manager/Officer* assists the System Owner in ensuring separation of duties for accounts including permissions and profile sets within the system; CFPB staff and contractors must submit privileged user agreement (PUA) requests, which are approved by the System Owner before access is granted to the CRS; *Consumer Guides* have limited access to the system to enter data for a complaint; all authorized users are restricted to the minimum amount of data required to carry out their assigned job responsibilities);
- Physical perimeter security safeguards;
- Risk and controls assessments and mitigation;
- Security Operations Center to monitor antivirus and intrusion detection software; and
- Records Schedule Submitted to National Archives and Records Administration: N1-587-12-05 and DAA-0587-2021-0002.

[22] Although pursuant to Section 1017(a)(4)(E) of the Consumer Financial Protection Act, Pub. L. No. 111-203, the CFPB is not required to comply with Office of Management and Budget (OMB)-issued privacy guidance, its intention is to voluntarily follow OMB privacy-related guidance as a best practice and to facilitate cooperation and collaboration with other agencies.

The CFPB provides limited access to authorized personnel, including employees and contractors acting on its behalf who have a need to know the information. It also provides its employees with appropriate privacy and security training to ensure information is used and secured appropriately, including specialized training for CRC contractors. Procedures to terminate or restrict access for individuals are in place once they no longer have a need to access information in the CRS such as because of a termination, resignation, or no longer having a need to know for their assigned job duties.

The CFPB has updated this PIA as a result of its privacy continuous monitoring (PCM) processes. The system has also been assessed to determine how it provides a secure and automated approach to business operations. As documented in this PIA, the CFPB has confirmed suspected breach notification processes and plans and secure channels for submitting transactional information. As a result of performing assessments documented in this PIA update, the CFPB provides additional privacy guidance and training to internal and external portal users on how to safeguard PII and report suspected privacy breaches. Consumer Response has established restrictions for complaint export through Complaint Explorer to limit the amount of complaint data that leaves the CRS to the minimum amount necessary. Consumer Response has also strengthened user agreements to ensure that complaint data is only exported when there is an authorized need and is securely disposed of when no longer needed for approved business. Additionally, the CFPB has issued an ATO for the CRS and for Complaint Explorer, affirming compliance with federal and CFPB protocols regarding security and privacy.

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.)

As required by the Act, Consumer Response developed procedures with other federal, state, and local government agencies to provide responses to consumers and share information. Consumer PII accompanies the sharing of complaints with the other agencies.[23] For example, Consumer Response shares information with the FTC to coordinate their enforcement of consumer

[23] For a list of the types of agencies and entities CFPB shares information with please review, CFPB.005—Consumer Response System SORN.

protection laws. Consumer Response has data sharing agreements in place with these entities for sharing CRS data. Consumer Response only shares that information through secure channels in processes governed by data sharing agreements.

User access to the CRS is also granted through PUA requests or onboarding access requests for the Company, Government, and Congressional portals. For the Company Portal, companies designate at least one authorized POC during the company onboarding process. After a company is onboarded, authorized company POCs can grant other company representatives' access to the portal by creating a user account through their own portal account. Authorized company POCs are also responsible for removing account access when users no longer need access. The CRS requires Company, Government, and Congressional portal users to provide username and password, and use multi-factor authentication for access.

For Government Portal users, including those accessing Complaint Explorer, there is authenticated access and there are technical safeguards to minimize risk of use, disclosure, or retention of information. Government Portal authorized representatives certify that their agencies agree to the terms of use for the Government Portal Agreement and attest that all users of the agency will follow the requirements to protect PII. All users individually attest that they agree with CFPB requirements to safeguard PII each time they log in to the Government Portal to access Complaint Explorer.

All Government Portal users receive instructions to protect PII each time that they access the Government Portal and individually agree to the requirements of the Government Portal They also receive reminders when accessing Complaint Explorer. Government Portal authorized representatives sign the Government Portal Agreement and POCs certify for their agencies that users will follow the rules of behavior while using the Government Portal and Complaint Explorer and will follow all CFPB requirements to protect PII.

Document control

Approval

CHRISTOPHER CHILBERT
Digitally signed by CHRISTOPHER CHILBERT
Date: 2024.08.19 17:04:28 -04'00'

Chris Chilbert

Chief Information Officer

KATHRYN FONG
Digitally signed by KATHRYN FONG
Date: 2024.08.19 19:30:50 -04'00'

Kathryn Fong

Chief Privacy Officer

CHRISTOPHER JOHNSON
Digitally signed by CHRISTOPHER JOHNSON
Date: 2024.08.16 14:13:16 -04'00'

Christopher Johnson

Initiative Owner

Change control

Version	Summary of material changes	Pages affected	Date of change
1.0	Initial Publication	All	March 2013
2.0	Revision and reorganization of document.	All	August 2024