Consumer Response - Consumer Resource Center (CRC)

s

Does the CFPB use the information to benefit or make a determination about an individual?	Yes
What is the purpose?	Collect and process data to facilitate contact center services and improve user experience. products, services, and entities.
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.

Overview

The Dodd-Frank 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 or Bureau). The Bureau administers, enforces, and implements federal consumer financial protection laws, and, among other powers, has authority to protect consumers from unfair, deceptive, and abusive practices related to consumer financial products or services.

One of the primary functions of the Bureau under the Dodd-Frank Act is collecting, investigating, and responding to consumer complaints.[1] The Bureau is also tasked with analyzing complaints to identify trends in service delivery to consumers. To fulfill these obligations, the Bureau created the Office of Consumer Response (Consumer Response) to:

- Answer consumers' questions
- Handle consumers' complaints
- Analyze and share complaint data and insights

Consumer Response engages directly with consumers to understand the challenges they face in the financial marketplace and responds to their inquiries about consumer financial products and services. Consumer Response receives complaints about financial products and services from consumers via the Bureau's website, ConsumerFinance.gov/complaint/, by phone, physical mail, and email.[2] In addition, the Bureau receives complaints by referral from other government agencies, the White House, and Congressional offices.

In addressing a complaint or inquiry, Consumer Response may provide additional information to the consumer, send the complaint to the company or financial service provider that is the subject of the complaint, refer the complaint to another government agency, or direct the submission to other offices in the Bureau for further administrative action.

[1] 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.

[2] As an operational matter for the purposes of establishing reasonable procedures for providing timely responses to consumer inquiries, the Bureau defines consumer inquiries as consumer requests for information—typically proffered by telephone—to its Office of Consumer Response about consumer financial products or services, the status of a complaint, an action taken by the Bureau, and often combinations thereof.

The consumer complaints or inquiries themselves (including records about the complaint, details and supporting documents/documentation) are collected by Consumer Response and maintained in the Consumer Response System (CRS), which is the Bureau system of record for these interactions.[3]

Consumer Response, with vendor assistance, operates the Consumer Resource Center (CRC), to directly interact with consumers for the intake of complaints and to field inquiries. While the vendor supports intake by phone, its services also include intake of physical mail[4] and email. To do this, the vendor provides contact center services with Consumer Guides[5] who work at both a secure physical location and remotely.

The contact center provides the following services and capabilities:

- Communicate with consumers using a variety of telephony services;[6]
- Scan and print documents submitted by consumers;
- Perform quality assurance (QA) reviews of data entered by Consumer Guides as they process documents and interact with consumers;
- Train Consumer Guides; and
- Facilitate workforce management (WFM) of Consumer Guides to ensure sufficient staffing to support services and capabilities.[7]

[3] For more information, please see the Consumer Response PIA, March 2013, found here: https://files.consumerfinance.gov/f/201303_CFPB_PIA-Consumer-Response-System.pdf.

[4] This refers to digitization of physical mail, where complaints and other documents are sent by consumers to a designated Bureau address for the CRC, processed by vendor staff and immediately scanned into CRS for Bureau use and documentation.

[5] Consumer Guides are vendor staff working behalf of the Bureau, who are trained to process complaints and inquiries from consumers. They interact directly with consumers if they choose to speak to a person when calling the CRC contact center.

[6] Telephony refers to technology that facilitates communication over long distances through voice, text messages, video calling and conferencing, voicemail, call recording and fax. Specifically, when considering voice, this PIA refers to real time voice communications and their capture, including caller self-service, call routing for assisted services, call recording, and similar voice-type services.

[7] WFM uses PII for identity verification of staff and the overall operation of the CRC. For example, the email of Bureau staff is used for authentication to obtain access to the CRC system to fulfill their duties.

The services provided by the vendor are conducted in a secure physical location and within a FedRAMP[8] compliant private cloud environment that connects with the Bureau's CRS for direct input, transmission, and viewing of consumer information.

During its activities processing complaints, the CRC and the applications that support its operations collect, process, store, and transmit consumers' submissions, which can include the consumers' personally identifiable information (PII) and PII of financial service providers, and its employees, as well as that of Bureau and vendor staff. Among the expected PII that can be transmitted through the CRC are names, email addresses, mailing addresses, phone numbers, official identification numbers, copies of documents/records, and details provided by consumers in their complaints (i.e., account numbers, transaction information, etc.). The collection, input, and storage of consumer information by the CRC is confined solely to the Bureau and vendor systems that compose the CRC. The CRC uses automated features, some of which feature artificial intelligence technology[9] to capture and process data (including PII) from its activities to monitor and enhance its operations. This information includes metadata related to a consumer call received by the CRC, such as the date and time call was received, call time duration, how long a consumer was on hold, and the outcome of the call.

Consumer complaint information and data (i.e., the contents of a complaint) is stored in the Bureau's CRS, with limited access to non-Bureau staff. Consumer Guides working in the CRC environment connect to the CRS to enter information collected from consumers and to access the information needed to assist the individual consumers they are helping. The data documenting operations performance of processes is collected by CRC systems to inform the development of comprehensive and efficient support for consumers, while deriving insights for improving user experience. For transparency and reporting purposes, de-identified, aggregate CRC data may be published and analyzed for public use.

The Bureau is publishing this Privacy Impact Assessment (PIA) to assess privacy risks associated with the collection and use of PII by CRC systems. The scope of the PIA is limited to

---

[8] Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

[9] Tools include enhanced processing of voice communications such as interactive voice response (IVR) - a technology that allows humans to interact with a computer-operated phone system using voice and natural language processing - the automatic computational processing of human languages. Advanced data analytics is a used to assess performance and distill operation improvements.

contact center services and associated technologies provided by the vendor. The privacy risks and mitigation efforts associated with the collection, use, and maintenance of consumer complaint, inquiry, and feedback data within the CRS is documented separately, in the Consumer Response PIA [10]

Information collected from the activities described in this PIA are covered under the System of Records Notice (SORN), CFPB.005, *Consumer Response System.* The collection of information is covered under the Paperwork Reduction Act (PRA), which is covered under OMB Control Number, OMB #3170-0011.

Privacy Risk Analysis

This PIA considers the privacy risk for contact center services of the CRC. These risks are assessed generally across the system. Where relevant, risks associated with specific functions, transactions, or interactions with consumers are noted.

The following risk categories apply generally across the CRC:

- Limits on Uses and Sharing information
- Security
- Awareness and Training
- Data quality and integrity

Limits on Uses and Sharing of Information

There is a risk that unauthorized third parties may use contact center services to obtain information about a consumer or complaint that is not theirs. To mitigate this, CRC services employs validation processes to ensure that individuals who request information about a complaint or inquiry are properly verified. This is done when individuals are required to provide different forms of identification or security verifications prior to obtaining access. When speaking to consumers Consumer Guides handling calls are required to obtain verification of identity prior to providing any information about a complaint or inquiry. Access controls, along

[10] See Consumer Response PIA, March 2013.

with other privacy controls are in effect with CRC to limit access to sensitive information only those who are authorized due to their role and a need to know.

Security

In supporting the operation to field and process complaints or inquiries from consumers, CRC utilizes PII, which is entered into Bureau systems. This information is a target for hackers, identity thieves, and other threats. The Bureau has mitigated this vulnerability by implementing appropriate security controls to protect information contained in the systems against unauthorized disclosure and access.

Only authorized users (i.e., consumers who are involved in a complaint, Bureau staff, and support staff) have access to the CRC system, with access limited to the role served in the process. Bureau and vendor staff users are restricted to the minimal amount of data needed to carry out their assigned job responsibilities. The Bureau terminates or reduces access of an employee or contractor if they no longer have a need to know the information, resign, or are terminated.

The Bureau has emergency plans and incident-reporting procedures for security incidents involving the CRC. The Bureau, vendor, and a third-party quality assurance service monitor daily use of the system for suspicious or possible inappropriate activity. They are responsible for reporting any incidents and coordinating escalation, reporting, and response procedures to the Bureau.

Awareness and Training

Receiving consumer complaints and inquires is a critical function of the Bureau, with the collection and use of PII a necessity to its mission. In the course of this work there is a risk that CRC staff may inadvertently mishandle the PII it collects from consumers, by sharing it with an unauthorized person due to a gap in knowledge of Bureau procedure.

To ensure that this risk is mitigated, CRC staff are required to complete annual role-based training on handling data and information security. Internal rules and guidance for managing PII apply to all who work for the Bureau, including vendor staff. The training includes recognizing possible breaches of PII and how to report them.

Data Quality and Integrity

During CRC operations, the Bureau needs to ensure that the data collected in the processing of a complaint or inquiry is accurate upon capture and remains so throughout its lifecycle. There is a privacy risk that incorrect information about the consumer is captured during their interaction

with the contact center, which can result in future communications being sent to someone who is not party to the complaint/inquiry or delays in the processing their submission.

To mitigate this risk, the consumer can contact the Bureau through the CRC to correct or amend records about themselves. Additionally, under the Privacy Act of 1974, an individual can submit a request to amend or correct their record, either directly or through a request made by their legal representative or their Congressional representative. Information about Privacy Act requests is available in the SORN, CFPB.005 – Consumer Response System, and at https://www.consumerfinance.gov/foia-requests/.

The following risk categories apply to specific parts of the consumer complaint, inquiry, and feedback processes:

- Data Minimization
- Individual Participation

Data Minimization

Consumer Interactions
During an interaction with the contact center there is a risk that a consumer may disclose more information than necessary to a Consumer Guide for the service they are seeking.

To mitigate this risk, the CRC leverages processes and controls that limit the amount of information required to be provided by a consumer. For example, when a consumer calls the CRC for a status update on a complaint, the Consumer Guide asks for basic, non-sensitive information to verify the consumer's identity. The Consumer Guide does not ask for Social Security Numbers (SSN) or other sensitive information to verify one's identity for services that do not need it. Additionally, when intaking a complaint, the Consumer Guide is trained to only ask for the necessary information to complete the complaint form. In some cases—and in compliance with record management requirements to limit the amount of sensitive information held by the Bureau, the Bureau may not collect or will immediately delete certain sensitive information (e.g., account numbers) that a consumer provided to CRC systems, if it is not needed for that service.

Individual Participation

There is a privacy risk that consumers are unaware of the information the Bureau maintains about them in order to process a complaint. Notice and consent of use is employed to mitigate this risk. The Bureau informs consumers who engage the CRC that the disclosure of personal information is voluntary. Additionally, the Bureau provides Privacy Act Statement and other forms of notice (including this PIA) detailing how the consumer's information is collected by the CRC is used.

Consumer submissions by third parties

There is a risk that complaints could be submitted on behalf of consumers without their consent, using the contact center system. Entities generally cannot share consumers' financial information—including as part of the complaint process—unless everyone listed in the complaint is also listed on the account or loan or authorized by the customer to receive financial information. Entities may require that their customers provide signed, written permission directly to them before sharing financial information with a third party, such as a lawyer, guardian, or a person with power of attorney.

With these mitigation procedures in place, 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 CRC collects PII directly from consumers who engage it to submit complaints or make inquiries to the Bureau.[11] This may be done by Consumer Guides who intakes a consumer complaint or inquiry via telephone and enters the information into the CRS. Alternatively, the CRC may receive information directly provided by consumers through other means, such as receiving a complaint or inquiry through physical mail or electronic submission. The PII collected by the Consumer Guides or taken in by the CRC varies and the consumers can choose the type and amount of identifying information they include when submitting a complaint.

The information typically captured includes:[12]

- Consumer's name;
- Contact information (e.g., address, email address, telephone number);
- Name of financial service provider or regulated entity;
- Description of what happened;
- Desired resolution;
- Product, sub-product, issue, and sub-issue and related sub questions;
- Miscellaneous scanned files/documents related to the complaint; and
- Voice data/voice recordings.

Additional information may be requested in order to process the submission.

When consumers call the Bureau's toll-free telephone number, they initially engage with an automated interactive technology to begin directing them to the appropriate service. This is also where they may begin to provide their personal information. Depending on their selection, consumers using this technology can be directed to answers for common questions about relevant consumer financial products and educational content.

Some consumers opt to engage a Consumer Guide. Consumer Guides are vendor employees working on behalf of the Bureau, that are trained to answer inquiries and handle complaints.

---

[11] The CRC is an exclusive vendor operated private environment for the Bureau (in compliance with FedRAMP), which is directly connected to the CRS and Bureau systems for data entry and transfer. Federal and contractual requirements require the CRC employ the risk mitigation strategies detailed here to address risks operational risks from the vendor.

[12] For more information on how consumer complaint data is maintained and used, please see the Consumer Response PIA, March 2013: https://files.consumerfinance.gov/f/201303_CFPB_PIA-Consumer-Response-System.pdf.

CRC staff either work remotely or are based at secure physical locations managed by the vendor. They are also subject to various security requirements such as background checks, training, and access controls. Consumer Guides are prohibited from retrieving or storing any information from Bureau systems beyond their scope of work. The vendor utilizes a VoIP (voice over Internet Protocol) telephony technology, that connects to the CRS, allowing Consumer Guides to perform their work and enter information provided by the consumer directly in the CRS system.

CRC systems also support mail operations, where vendor staff process physical mail, directly scanning copies into the CRS for further evaluation. CRC systems capture an image of the documents from the scan and create metadata (i.e., date scanned) that accompanies the file which is sent. The image of the scanned doc is deleted from the CRC and stored in CRS.

CRC provides features such as IVR, natural language processing, call recordings, and advanced data analytics that are embedded in these systems and leveraged by CRC to streamline operations, collect data, and process it for enhanced functionality and improvement of user experience. These tools do not require the collection of additional PII to function; rather, they utilize information that is already collected as part of a call. For example, the capture of voice recordings or analysis of metadata about a call made to the contact center (e.g., length of call, how long caller was on hold) is used for this purpose. Call recordings are captured and temporarily stored in the CRC, to be eventually transferred to the CRS for secure data storage.

Complaint status confirmation
Consumers can obtain the status of their complaint submission and the company's response through via telephone. To do this, consumers call the CRC and verify their identity (e.g., confirming their email address, phone number, mailing address, complaint number, etc.) to check the status of their complaint submission.

2. Describe CFPB's objective for the information.

The CRC uses the PII it collects for two primary reasons to process complaints or answer inquiries from consumers and to gain insight for advancements in user experience and overall CRC operations. The CRC, in accordance with Bureau policy collects only what is necessary for these purposes. Access to the PII that is generated from the CRC is limited to those who are party to an inquiry or complaint or those who are assisting in processing it. The data collected by the CRC is confined to Bureau and vendor systems. Third parties outside of those involved in the complaint/inquiry, the vendor, or the Bureau do not have access to this data. Consumers can

obtain the status of their complaint submission and the company's response through via telephone. To do this, consumers call the CRC and verify their identity (e.g., confirming their email address, phone number, mailing address, complaint number, etc.) to check the status of their complaint submission.

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.

The Bureau collects PII, including voice recordings and details of a complaint/inquiry in the CRC environment and enters it into the CRS to form the contents of a complaint or inquiry.[13] The Bureau makes available information that is collected by CRC to other government agencies (including state and local) who may have jurisdiction to issues in a complaint. These entities must be registered with the Bureau and are subject to data sharing and use agreements, federal law, and other regulations that protect PII. Access to this information by other agencies is through the Government Portal, which is a secure, web-based channel through which the government agency can view consumer complaints and related data received in the CRC.

The Bureau shares limited information with Congressional offices and the White House through a Congressional Portal. Congressional offices that complete applicable onboarding and privacy forms can view complaints they submit on behalf of their constituents for which they provide consumer-signed privacy releases. The White House refers complaints to the Bureau and information is shared per agreement.

In some cases, the Bureau is legally required to share CRC data. Any disclosure of PII is done in accordance with the routine uses published in CFPB.005 Consumer Response SORN.

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)

[13] Though not PII, metadata from operations is generated by the system and leveraged by the Bureau to assist in processing complaints when needed or for CRC administrative purposes.

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

The Bureau provides notice to consumers about how their information will be collected and used through this PIA, the associated CFPB.005 – Consumer Response SORN, and Privacy Act Statements. Consumers are informed that providing their personal information when making a submission is voluntary. At their discretion, consumers can limit the amount of PII disclosed to the Bureau in their submission. Additionally, the Bureau provides an automated privacy notice to consumers when they call into the CRC and advises consumers that calls may be monitored and recorded.

The Bureau gives consumers the ability to request access and amendment to their personal information in accordance with the Privacy Act and the Bureau'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 its behalf—collection, use, disclosure, retention, or disposal of information.

The Bureau manages risks to privacy by complying with the Privacy Act of 1974, Right to Financial Privacy Act, and E-Government Act of 2002. To further compliance, it voluntarily adopts Office of Management and Budget privacy-related guidance as best practice[14] and applies National Institute of Standards and Technology risk management processes for privacy.

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

The Bureau uses the following technical and administrative controls to secure the data and provide accountability for the appropriate collection, use, disclosure, and retention of personal information:[15]

- Personnel security including background checks
- Mandatory Bureau information security awareness training
- Mandatory Bureau privacy awareness training
- Audit logs and reviews
- Implementing the CFPB Privacy Breach Response and Recovery Plan
- Compliance with CFPB Cybersecurity Policy and Procedures
- Data Quality and Integrity Checks
- Data encryption
- Extract logging
- Procedures and guidance
- Role-based Access Controls
    - Consumer Guides – use of telephony solutions, limited access to CRS, scanning solution
    - Team Lead – access to CRC and vendor contact solution
    - Report Analyst (up to two employees) – access to CRS and vendor contact solution
    - Contact Center Manager/Supervisor (up to six vendor employees) – access to all vendor side CRC systems to perform duties
    - Training staff – access to all systems to perform duties
    - Quality Analyst – access to all systems to perform duties
    - Quality Manager – access to all systems to perform duties
    - Contact Security Specialist (CSS) – access to all systems to perform duties
    - Program Manager (up to two full-time Bureau employees) – access to all systems in CRC to perform duties
- Records Schedule Submitted to National Archives and Records Administration under: N1-587-12-05 and N1-587-12-04

Authorized personnel, including employees and contractors acting on its behalf, are issued access to the Bureau systems to do their work. The Bureau provides both its employees and

[15] FedRAMP compliance and federal regulations for vendor operated cloud-based systems, require that risk mitigation protocols be in place. The strategies detailed reflect the implementation of these protocols by the vendor to address the risks they encounter.

contracted staff with appropriate privacy and security training to ensure information is used and secured appropriately. Contact center staff are also provided with enhanced training on handling sensitive information by the vendor. The Bureau also has procedures in place to terminate or restrict access for individuals who no longer have a need to access information in the CRC because of a termination or resignation.

Security controls for the CRC are leveraged to protect information contained in the system against unauthorized disclosure and access. Those controls are:

- Bureau policies, procedures, and guidance for privacy and information assurance
- Conducting background checks on personnel
- Initial and follow-on privacy and security awareness training for personnel
- Physical perimeter security safeguards
- Security Operations Center to monitor antivirus and intrusion detection software
- Risk and controls assessments and mitigation
- Technical access controls, such as role-based access management and firewalls

Disaster mitigation protocols for the CRC are present for catastrophic events and security challenges, like system outages. Those procedures include comprehensive data back-up for the CRC, breach notification processes, and secure channels for submitting transactional information.

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.)

CRC systems are used to provide a platform for the collection data from consumers that is directly entered into Bureau's CRS, to assist in the processing of their complaints and inquiries. Data from these activities also supports overall Consumer Response operations. While the vendor supporting CRC captures data and utilizes analytical tools developed by outside partners, any data captured from CRC activities is confined to vendor and Bureau systems and eventually deleted after being transferred directly to the Bureau. The vendor is also prohibited from sharing the data with outside entities.

Document control

Approval

CHRISTOPHER CHILBERT

Digitally signed by CHRISTOPHER CHILBERT
Date: 2021.12.03 13:45:35 -05'00'

Chris Chilbert

Chief Information Officer

Date

TANNAZ HADDADI

Digitally signed by TANNAZ HADDADI
Date: 2021.12.03 17:04:26 -05'00'

Tannaz Haddadi

Chief Privacy Officer

Date

Morgan M. Rogers

Digitally signed by Morgan M. Rogers
Date: 2021.12.03 12:17:05 -05'00'

Morgan Rogers

Section Chief of Stakeholder Services – Consumer Response

Date

Change control

Version	Summary of Material Changes	Pages Affected	Date of Change
1.0	New publication	All	12/1/21