UNITED STATES OF AMERICA
Before the
CONSUMER FINANCIAL PROTECTION BUREAU

In re	)
	)
Market Monitoring	)
Consumer Access to Personal Financial Data	)
	)

ORDER TO FILE INFORMATION

Pursuant to the Consumer Financial Protection Bureau's (Bureau's) authority under section 1022(c)(4)(B)(ii) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), 12 U.S.C. § 5512(c)(4)(B)(ii), Recipient Name is hereby ordered to file with the Bureau the information specified below.

Purpose

The Bureau is monitoring markets for risks to consumers associated with consumer access to personal financial data. This Order will provide information necessary to conduct such analysis in compliance with Congress' mandate that the Bureau monitor for risks to consumers in the offering or provision of consumer financial products or services, including developments in markets for such products or services. *See* 12 U.S.C. § 5512(c)(1).

This is a market-monitoring order issued under section 1022(c)(1) & (4) of the Dodd-Frank Act, 12 U.S.C. § 5512(c)(1) & (4). It is not a supervisory order issued under sections 1024 or 1025 of the Dodd-Frank Act, 12 U.S.C. §§ 5514 or 5515.

The Bureau is engaged in an ongoing rulemaking process relating to personal financial data rights. Most recently, the Bureau published an "Outline of Proposals and Alternatives Under Consideration" in accordance with the requirements of the Small Business Regulatory Enforcement Fairness Act of 1996. That outline can be found at https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf. Information provided in response to this Order is intended to be used in support of the Bureau's ongoing rulemaking efforts around personal financial data rights, although the Bureau reserves the right to use the information for any purpose permitted by law.

Order Terms and Procedure

The information required by this Order must be filed pursuant to the terms of this Order, including the stated Instructions and Definitions. Responses are required to all questions listed below and in all attachments to this Order.

Timely responses to the request are legally required. *See* 12 U.S.C. § 5512(c)(4)(B)(ii). Responses are due on or before 5:00 PM Eastern time, March 27, 2023. The instructions below contain more information about how to submit your responses.

As indicated below, you should contact the Bureau as soon as possible if you have any questions about the terms of the Order or the procedure for responding to it.

The Bureau will treat the information received in response to this Order in accordance with its confidentiality regulations at 12 CFR § 1070.40 *et seq*.

It is so ordered.

[SIGNED]
DATE: January 25, 2023

Instructions

1. Until you are notified otherwise, retain—and suspend any procedures that may result in the destruction of—all documents, information, and tangible things that are in any way relevant to responding to this Order.
2. Submit your responses with an accompanying affidavit or declaration, made by one or more officers of COMPANY who are authorized to represent COMPANY, affirming that the information is true and accurate and does not contain any omissions that would cause the responses to be materially misleading.
3. Submission will be made to the Bureau via a Secure File Transfer Protocol (SFTP) server unless COMPANY and the Bureau agree in writing to another method. Connection information will be provided. COMPANY is responsible for ensuring connectivity to the SFTP server from its environment. Any questions about method of transfer should be discussed in advance with the Bureau.
4. Do not include any personally identifiable information that directly identifies any consumer, such as a consumer's name, address, telephone number, Social Security number, or unhashed account number.
5. Unless otherwise specified, the questions seek information about the Relevant Period (as defined below).
6. Provide a full, separate response for each question and sub-question asked.
7. Please submit all responses in writing, in a machine-readable format.
8. Files containing the information requested by the Order must be uploaded to the SFTP server on or before 5:00 PM Eastern time, March 27, 2023.
9. The Bureau may issue follow-up requests in connection with your responses.
10. If you have questions about the information requested by the Order, please contact the Bureau as soon as possible to schedule a meeting on or before February 17, 2023 to resolve such questions. During this meeting, you must be in a position to attempt to resolve all issues regarding the Order. Be prepared to discuss your planned compliance schedule, including any proposed changes that might reduce your cost or burden while still giving the Bureau the information it needs.

Definitions

For purposes of the Order:

1. "COMPANY," "you," or "your" means Recipient Name and any parent companies, wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all principals, directors, officers, owners, employees, agents, representatives, consultants, attorneys, accountants, independent contractors, and other persons working for or on behalf of the foregoing.
2. "Relevant Period" means January 1, 2019 through December 31, 2022.
3. "Consumer portal" means an electronic system which you have developed and deployed, or contracted to utilize, for the purpose of facilitating your consumer customers' ability to directly access personal financial data. This includes systems intended to be accessed via

web browser as well as systems intended to be accessed via dedicated applications developed for mobile or tablet operating systems.

4. “Permissioned third party” means any entity, other than COMPANY, which directly accesses your consumer portal(s) and/or your third-party portal(s) pursuant to a consumer’s permission to access that consumer’s personal financial data.
5. “Personal financial data” means information in your control or possession concerning any consumer financial product or service that a consumer obtains from you, including information relating to any transaction, series of transactions, or to an account including costs, charges and usage data.
6. “Screen scraping” means a practice by which a permissioned third party directly accesses a consumer’s personal financial data by accessing, on an automated basis, your consumer portal.
7. “Third-party portal” means an electronic system which you have developed and deployed, or contracted to utilize, for the purpose of facilitating permissioned third parties’ access to personal financial data. This includes application programming interfaces.

Questions

Instructions: if you contract with any service providers for the provision of your consumer and/or third-party portals, please describe their applicable roles, responsibilities, and activities in each response. Unless otherwise noted, please provide current information; if the answers to any question have changed significantly over the course of the Relevant Period, please note that as applicable.

Section A – Direct access

1. For which consumer financial products and services do you make personal financial data available to consumers in your consumer portals?
2. Are consumers able to download or extract personal financial data from your consumer portals, and if so in which formats? What is the scope of personal financial data consumers are able to download or extract? Do you track whether, how, and how frequently consumers use such functionality and, if so, what metrics do you use to track it?
    a. To the extent you maintain aggregate summary statistics in a readily-available form regarding consumers' downloading or extracting of personal financial data from your consumer portals during the Relevant Period, please provide such aggregate summary statistics.
3. Describe the standards you set for the reliability of your consumer portals, and the practices and programs you institute to achieve those standards. Specifically address:
    a. uptime, latency, and planned and unplanned outages; include in your response:
        i. the metrics you use to track uptime, latency, and planned and unplanned outages, if any; and
        ii. if you do use any such tracking metrics, please provide
            1. the actual average uptime and latency you achieved according to those metrics for each year in the Relevant Period; and
            2. the number, length, and/or impact of planned and unplanned outages, according to those metrics, for each year in the Relevant period;
    b. how you communicate planned outages to your consumers; and
    c. how you address planned and unplanned outages, including whether and how you make personal financial data available to consumers by other means.
4. Describe the cost of providing your consumer portals, including staff hours and other costs.
5. Describe how you track enrollment in and utilization of your consumer portals, including any metrics you use to track consumers' utilization of consumer portals (including but not limited to tracking of access attempts and amounts of data provided or bandwidth utilized).

a. To the extent you maintain aggregate summary statistics in a readily-available form regarding enrollment in, and utilization of, your consumer portals during the Relevant Period, please provide such aggregate summary statistics.

Section B – Screen scraping

6. How many permissioned third parties access personal financial data via screen scraping?
7. Describe how permissioned third parties access personal financial data via screen scraping. Specifically:
    a. which consumer portals are accessed via scraping by permissioned third parties;
    b. how you identify permissioned third parties who scrape your consumer portals;
    c. how you know which data are being requested; and
    d. what policies or other measures you implement to regulate screen scraping.
8. Describe the cost of managing screen scraping on your consumer portals, including staff hours and other costs.
9. Describe how you track the impact of screen scraping on the utilization of your consumer portals, including any metrics you use to track that impact, and whether and how you track the numbers of consumer accounts accessed via screen scraping.
    a. To the extent you maintain aggregate summary statistics in a readily-available form regarding screen scraping of your consumer portals during the Relevant Period, please provide such aggregate summary statistics.

Section C – Third-party portals

10. For each third-party portal you maintain, please describe:
    a. how many permissioned third parties access the portal;
    b. the products and services for which personal financial data are made available; and
    c. the technologies and systems you use to develop, implement, and maintain the portal.
11. Describe how permissioned third parties access personal financial data via your third-party portals. Specifically, for each third-party portal:
    a. describe the policies and procedures applicable to how an access attempt by a permissioned third party is authenticated, authorized, and serviced; and
    b. describe any limitations on the use of personal financial data, other activity limitations, or other policies you require permissioned third parties to adhere to in order to access your third-party portals.
12. Are there any products and services, or data elements about such products and services, that you make available via your consumer portals, but do not make available via your third-party portals? If so, please identify those products or data elements and explain why.
13. List any personal financial data elements that you provide through your third-party portal only in masked, tokenized, or otherwise-altered form.
    a. Describe your reason for providing these elements in such altered manner.

b. Describe the policies and practices you maintain to ensure that such altered elements are equivalently usable by permissioned third parties to the unaltered data elements.

14. What recourse do you offer permissioned third parties if a third-party portal becomes unavailable? What is the process for permissioned third parties to exercise such recourse?
15. Describe the cost of providing third-party portals, including staff hours and other costs.
16. Describe how you track utilization of your third-party portals, including any metrics you use to track utilization of third-party portals (including but not limited to tracking of access attempts and amounts of data provided or bandwidth utilized).
    a. To the extent you maintain aggregate summary statistics in a readily-available form regarding utilization of your third-party portals during the Relevant Period, please provide such aggregate summary statistics.
17. Describe whether and how you track the numbers of consumer accounts accessed via your third-party portals.
    a. To the extent you maintain aggregate summary statistics in a readily-available form regarding the numbers of consumer accounts accessed via your third-party portals during the Relevant Period, please provide such aggregate summary statistics.

Section D – Standards for third-party portals

18. Do your third-party portals, in whole or in part, conform with any applicable industry standards? If so, name and describe those standards, and if your portals conform only in part, note where and why your portals diverge from conforming with a standard.
19. Describe the standards you set for the reliability of your third-party portals, and the practices and programs you institute to achieve those standards of reliability. Specifically address:
    a. uptime, latency, and planned and unplanned outages; include in your response:
        i. the metrics you use to track uptime, latency, and planned and unplanned outages, if any; and
        ii. if you do use any such tracking metrics, please provide
            1. the actual average uptime and latency you achieved according to those metrics for each year in the Relevant Period; and
            2. the number, length, and/or impact of planned and unplanned outages, according to those metrics, for each year in the Relevant period;
    b. if your reliability standards for your third-party portals differ from those for your consumer portals, explain how and why they differ, and whether you plan to align them; and
    c. the costs of implementing the standards described above.
20. How do you prevent fraudulent or unauthorized access to your third-party portals?

a. Describe how you resolve complaints from permissioned third parties that a given access attempt that you have denied as fraudulent or unauthorized is, in fact, legitimate.

21. Do you limit access to your third-party portals by permissioned third parties for reasons other than suspicion of fraud or unauthorized access? If so, explain the reason for such limitations, and how they are effectuated (for example, by capping access attempts).