Consumer Financial Protection Bureau

Table of Contents

Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

This document reflects the final rule as issued on March 30, 2023.

Although the document has been revised since that date, it has not been updated to reflect any effects of ongoing litigation involving the final rule. As a result of that ongoing litigation, the compliance dates in the final rule currently are stayed as to all covered financial institutions.

Small Business Lending Rule Info Sheet:

When must a financial institution begin collecting data and complying with the small business lending rule?

Generally, the small business lending rule (final rule) requires a financial institution[1] that is a covered financial institution for a given calendar year to collect data and otherwise comply with the final rule for that calendar year. Pursuant to the final rule, a financial institution is a covered financial institution for a given calendar year if it originated at least 100 covered originations in each of the two preceding calendar years. For example, a financial institution is a covered financial institution for 2026 if it had at least 100 covered originations for both calendar year 2024 and calendar year 2025.

However, as discussed below, not all covered financial institutions are required to begin complying with the final rule at the same time. This is because the final rule includes

---

This is a Compliance Aid issued by the Consumer Financial Protection Bureau. The CFPB published a Policy Statement on Compliance Aids, available at http://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/policy-statement-compliance-aids/, that explains the CFPB's approach to Compliance Aids.

[1] For purposes of the final rule, a financial institution is any partnership, company, corporation, association (incorporated or unincorporated), trust, estate, cooperative organization, or other entity that engages in any financial activity.

compliance date tiers that establish different initial compliance dates depending on the number of covered originations that a financial institution originated in 2022 and 2023. Thus, an important implementation step will be to determine the number of covered originations that a financial institution originated in 2022 and to determine the number of covered originations that the financial institution originates in 2023.

Generally, a covered origination is a covered credit transaction that the financial institution originates to a small business.[2] However, amendments, renewals, and extensions of existing transactions are not covered originations, even if they increase the credit line or credit amount of the existing transaction. If a financial institution does not have sufficient information readily available to determine if its originations for 2022 and 2023 were made to small businesses (as that term is defined in the final rule), the financial institution may use any reasonable method to estimate its covered originations for either or both of those two years. For instance, if a financial institution that does not have readily accessible information regarding which of its covered credit transactions were originated to small businesses prior to October 1, 2023, the financial institution can annualize its covered originations based on the number of covered credit transactions it originated to small businesses between October 1 and December 31, 2023 and use that annualized number to determine its covered originations for 2022, 2023, or both years. Also, as illustrated in the examples below, a financial institution may assume that all of the covered credit transactions it originated in 2022 and/or 2023 were made to small businesses.

The chart immediately below illustrates the compliance date tiers that financial institutions will need to consider when determining when they must begin collecting data and otherwise complying with the final rule.

Compliance date tier	Origination threshold for the compliance date tier	Date that a covered financial institution begins collecting data and otherwise complying with the final rule	Deadline for a covered financial institution to report first year of data to the CFPB
Tier 1	At least 2,500 covered originations	October 1, 2024	June 1, 2025

[2] Additional information about covered financial institutions, small businesses, covered credit transactions, and compliance dates is available in the Executive Summary of the Small Business Lending Rule, which is available at www.consumerfinance.gov/compliance/compliance-resources/small-business-lending-resources/small-business-lending-collection-and-reporting-requirements.

Compliance date tier	Origination threshold for the compliance date tier	Date that a covered financial institution begins collecting data and otherwise complying with the final rule	Deadline for a covered financial institution to report first year of data to the CFPB
	in both 2022 and 2023		
Tier 2	At least 500 covered originations in both 2022 and 2023 but not 2,500 or more covered originations in both 2022 and 2023	April 1, 2025	June 1, 2026
Tier 3	At least 100 covered originations in both 2022 and 2023 but not 500 or more covered originations in both 2022 and 2023	January 1, 2026	June 1, 2027
Additionally, even if it originated fewer than 100 covered originations in 2022 or 2023, a financial institution that originates at least 100 covered originations in 2024 and 2025 must collect data and otherwise comply with the final rule beginning January 1, 2026.			

The remainder of this info sheet discusses whether a financial institution must collect data and otherwise comply with the final rule for specific years.

Does my financial institution need to comply with the final rule for 2024?

A financial institution is only required to begin collecting data and otherwise complying with the final rule for 2024 if it meets the origination threshold for the Tier 1 compliance date. Thus, a financial institution must begin collecting data and otherwise complying with the final rule on October 1, 2024 if that financial institution originated at least 2,500 covered originations in both 2022 and 2023. If a financial institution is required to collect data for 2024, it must report that data to the CFPB by June 1, 2025. It must also comply with the final rule's other provisions,

such as the firewall provision and the recordkeeping provisions, with regard to the data collected for 2024.

The following flowchart may be used to help determine if a financial institution is required to collect data and otherwise comply with the final rule for 2024:

Example 1: Lender originates 2,600 covered originations in 2022 and 2,800 covered originations in 2023. Based on its 2022 and 2023 originations, Lender meets the origination threshold for the Tier 1 compliance date and is required to collect data and otherwise comply with the final rule beginning on October 1, 2024. It is required to report the data collected for 2024 to the CFPB by June 1, 2025.

Example 2: Lender has 2,000 covered originations in 2022 and 3,000 covered originations in 2023. Although Lender is a covered financial institution for 2024, it does not meet the origination threshold for the Tier 1 compliance date because it did not have at least 2,500 covered originations in 2022. Thus, it is not required to collect data or otherwise comply with the final rule for 2024. However, it must determine if it is required to collect data and otherwise comply for later years.

Example 3: In 2022, Lender originates 2,850 transactions that would be covered originations if they were made to small businesses, but Lender does not have sufficient

information readily available to determine whether the borrowers are small businesses pursuant to the final rule. Beginning on August 1, 2023, Lender begins asking applicants for business credit transactions whether they had gross annual revenue of $5 million or less in the applicant's prior fiscal year in order to determine if covered credit transactions originated between October 1 and December 31, 2023 are covered originations. Lender originates 650 covered originations between October 1 and December 31, 2023. Lender annualizes this number to determine that it originated 2,600 covered originations and applies this annualized number to 2022 and 2023. Because Lender determines that it originated 2,600 covered originations in both 2022 and 2023, Lender is required to collect data and otherwise comply with the final rule for 2024. It is required to report the data collected for 2024 to the CFPB by June 1, 2025.

Example 4: In 2022, Lender originates 1,900 transactions that would be covered originations if they were made to small businesses, but Lender cannot readily determine whether the borrowers were small businesses as defined in the final rule. Lender can assume that all 1,900 of its originations in 2022 are covered originations and use that number to determine that it does not satisfy the origination threshold for the Tier 1 compliance date. Regardless of how many covered originations it has for 2023, Lender does not satisfy the Tier 1 compliance date threshold because it did not have at least 2,500 covered originations for both 2022 and 2023. It is not required to collect data or otherwise comply with the final rule for 2024. However, Lender must determine if it is required to collect data and otherwise comply with the final rule for later years.

Example 5: In 2022, Lender originates 3,100 transactions that would be covered originations if they were made to small businesses. Lender obtains some information about applicants' gross annual revenue for these transactions but determines that it does not have sufficient information readily available to determine whether some of the transactions were made to small businesses as defined in the final rule. Lender collects all business credit applicants' gross annual revenue for transactions originated in 2023. Using this information, Lender determines that it originates 2,490 covered originations between January 1 and December 31, 2023. Regardless of the number of covered originations it had in 2022, Lender does not satisfy the origination threshold for the Tier 1 compliance date because it did not have at least 2,500 covered originations in both 2022 and 2023. It is not required to collect data or otherwise comply with the final

rule for 2024. However, Lender must determine if it is required to collect data and otherwise comply with the final rule for later years.

Example 6: Assume facts similar to those in example 5, above, except that Lender originates 2,510 covered originations in 2023. Lender may assume that all of the covered credit transactions it originated in 2022 were made to small businesses. If it does so, Lender satisfies the origination threshold for the Tier 1 compliance date and is required to collect data and otherwise comply with the final rule for 2024. Alternatively, Lender may use the number of covered originations it originates between October 1, 2023 and December 31, 2023 to determine its compliance date tier. Assume Lender originates 650 covered originations between October 1 and December 31, 2023. Using this number, Lender determines its annualized number of covered originations for 2022 is 2600 (650 x 4= 2,600). Using this annualized number of originations and its actual number of covered originations (i.e., 2,510) for 2023, Lender satisfies the Tier 1 compliance date threshold and is required to collect data and otherwise comply with the final rule for 2024. Finally, although the information is not readily available, Lender may decide to locate or obtain sufficient information to determine which of its 2022 covered credit transactions were made to small businesses. Assume Lender locates or obtains sufficient information to determine that it had no more than 2,499 covered originations for 2022. In this case, Lender does not satisfy the Tier 1 compliance date threshold because it did not originate at least 2,500 covered originations in 2022. Although it is not required to collect data or otherwise comply with the final rule for 2024, it must determine if it is required to collect data and otherwise comply with the final rule for later years.

Example 7: Lender originates 75 covered originations in 2023. Regardless of the number of covered originations it had in 2022, Lender is not required to collect data or otherwise comply with the final rule for 2024, but it must determine if it is required to collect data and otherwise comply for later years.

Does my financial institution need to comply with the final rule for 2025?

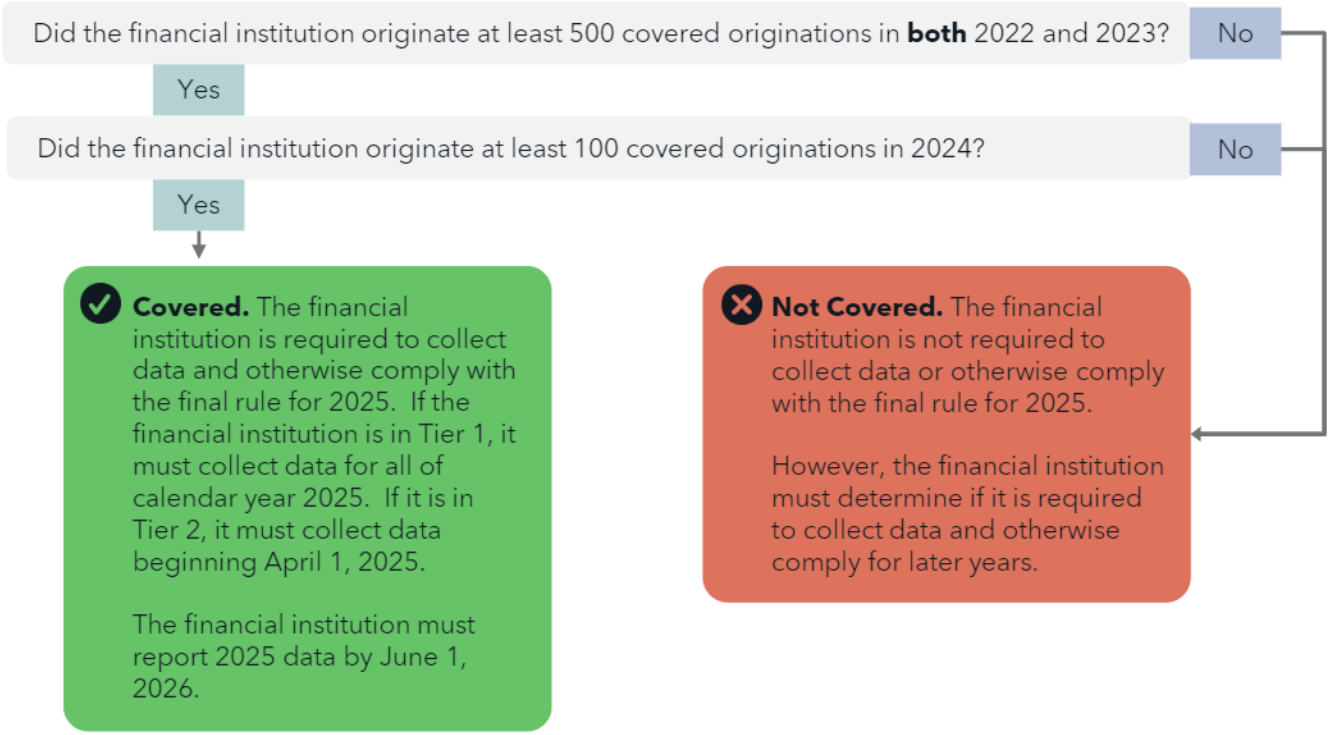
If a financial institution that is required to collect data and otherwise comply with the final rule for 2024 (i.e., the financial institution meets the origination threshold for the Tier 1 compliance date) originates at least 100 covered originations in 2024, it must collect data for all of calendar year 2025 and otherwise comply with the final rule for 2025. Among other things, it must collect data for calendar year 2025 and report that data by June 1, 2026. It must also comply with the final rule's other provisions with regard to the data collected for 2025. Conversely, if a financial institution that is required to collect data and otherwise comply for 2024 does not originate at least 100 covered originations in 2024, the financial institution is not a covered financial institution for 2025. It must report the data it collected in 2024 by June 1, 2025, but it is not required to collect data for 2025.

If a financial institution is not required to collect data or otherwise comply for 2024, it must begin collecting data and otherwise complying with the final rule on April 1, 2025 if it:

- **Meets the origination threshold for the Tier 2 compliance date.** This means that it originated at least 500 covered originations in both 2022 and 2023; and
- **Meets the origination threshold to be a covered financial institution for 2025.** This means that it originated at least 100 covered originations in 2023 and 2024.

If a financial institution is required to collect data for 2025, it must report that data to the CFPB by June 1, 2026. It must also comply with the final rule's other provisions with regard to the data collected for 2025.

The following flowchart may be used to help determine if a financial institution is required to collect data and otherwise comply with the final rule in 2025:



Example 1: Lender originates 520 covered originations in 2022, 510 covered originations in 2023, and 420 covered originations in 2024. Based on its 2022 and 2023 originations, Lender does not meet the origination threshold for the Tier 1 compliance date, but does meet the origination threshold for the Tier 2 compliance date. Additionally, Leder meets the origination threshold to be a covered financial institution for 2025. Thus, Lender is required to begin collecting data for 2025 on April 1, 2025 and otherwise complying with the final rule on April 1, 2025. Lender is required to report its 2025 data to the CFPB by June 1, 2026.

Example 2: Lender originates 510 covered originations in 2022, 502 covered originations in 2023, and 99 covered originations in 2024. Although Lender meets the origination threshold for the Tier 2 compliance date, it does not meet the origination threshold to be a covered financial institution for 2025. It is not required to collect data or otherwise comply with the final rule for 2025. However, it must determine if it is required to collect data and otherwise comply for later years.

Example 3: In 2022, Lender originates 510 transactions that would be covered originations if they were made to small businesses, but Lender does not collect information sufficient to determine whether its borrowers are small businesses as defined in the final rule. Lender begins asking applicants whether they had gross annual revenue of $5 million or less in the applicant's prior fiscal year in order to determine if the transactions it originates on or after October 1, 2023 are covered originations. Lender determines that it originated 147 covered originations between October 1 and December 31, 2023. Lender annualizes this number to determine that it originated 588 covered originations and applies this annualized number to 2022 and 2023. Lender originates 485 covered originations in 2024. Because Lender determines that it originated 588 covered originations in both 2022 and 2023, Lender meets the origination threshold for the Tier 2 compliance date. Because Lender determines that it originated 588 covered originations in 2023 and 485 covered originations in 2024, it meets the origination threshold to be a covered financial institution for 2025. It is required to collect data for 2025 and otherwise comply with the final rule beginning on April 1, 2025. It must submit its 2025 data to the CFPB by June 1, 2026.

Example 4: In 2022, Lender originates 215 transactions that would be covered originations if they were made to small businesses, but Lender does not collect information sufficient to determine whether an applicant is a small business pursuant to the final rule. Lender assumes that all 215 transactions are covered originations. Regardless of the number of covered originations it has for 2023, Lender does not satisfy the origination threshold for the Tier 2 compliance date and is not required to collect data or otherwise comply with the final rule for 2025. However, it must determine if it is required to collect data and otherwise comply for later years.

Example 5: Lender originates 85 covered originations in 2022, 90 covered originations in 2023, and 105 covered originations in 2024. Lender does not meet the origination threshold to be a covered financial institution for 2025 and is not required to collect data or otherwise comply with the final rule for 2025. However, it must determine if it is required to collect data and otherwise comply for later years.

Example 6: Lender is a new company and begins originating covered credit transactions in 2023. It originates 525 covered originations in 2023 and 550 covered

originations in 2024. Because Lender did not have any originations in 2022, it does not satisfy the origination threshold for the Tier 2 compliance date and is not required to collect data or otherwise comply with the final rule for 2025. However, it must determine if it is required to collect data and otherwise comply for later years.

Does my financial institution need to comply with the final rule for 2026 or later years?

For 2026 and later years, the final rule does not have separate origination thresholds for compliance date tiers and institutional coverage. Instead, a financial institution must comply for a given calendar year if it satisfies the general origination threshold for that year (i.e., the financial institution originated at least 100 covered originations in both of the two immediately preceding calendar years). Thus, if a financial institution satisfies the origination threshold to be a covered financial institution for 2026 or for a later year, the financial institution must comply with the final rule for that year. It must collect data for the calendar year and report that data by the following June 1. It must also comply with the final rule's other provisions with regard to the data collected.

For example, if a financial institution originates at least 100 covered originations in both 2024 and 2025, it is a covered financial institution and is required to collect data for 2026 and otherwise comply with the final rule for calendar year 2026. The covered financial institution must report to the CFPB the data collected in 2026 by June 1, 2027.

Similarly, a financial institution that originates at least 100 covered originations in both 2025 and 2026 is a covered financial institution for 2027. It must collect data for calendar year 2027 and report that data to the CFPB by June 1, 2028. It also must otherwise comply with the final rule with regard to the data collected for 2027.

The following flowchart may be used to help determine if a financial institution is required to collect data and otherwise comply with the final rule for 2026 or later years:

Example 1: Lender originates 490 covered originations each year between 2022 and 2025. Based on the compliance date tiers in the final rule, Lender is not required to collect data or otherwise comply with the final rule until January 1, 2026. It must collect data for 2026, report its 2026 data to the CFPB by June 1, 2027, and otherwise comply with the final rule for 2026. If Lender originates at least 100 covered originations in 2026, it will also be a covered financial institution and required to collect data for 2027 and otherwise comply with the final rule for 2027.

Example 2: Lender originates 85 covered originations in 2022, 90 covered originations in 2023, 105 covered originations in 2024, and 95 covered originations in 2025. Lender is not a covered financial institution and is not required to collect data or otherwise comply with the final rule for 2024, 2025, or 2026. Additionally, because Lender did not originate at least 100 covered originations in 2025, it will not be a covered financial institution and will not be required to collect data or otherwise comply with the final rule for 2027. However, it must determine if it is required to collect data and otherwise comply for later years.

Example 3: In 2022, Lender originates 145 transactions that would be covered originations if they were made to small businesses and assumes that all 145 transactions are covered originations. Because it did not originate at least 500 covered originations in 2022 and 2023, the earliest that Lender could be required to collect data and otherwise comply with the final rule is January 1, 2026. Lender begins asking all applicants for business credit for their gross annual revenues beginning in October 2023 and is able to determine if applicants are small businesses for all covered credit transactions originated on or after January 1, 2024. Lender originates 125 covered originations in 2024 and 95 covered originations in 2025. Lender is not a covered financial institution and is not required to collect data or otherwise comply with the final rule for 2024, 2025, or 2026. Additionally, because Lender did not originate at least 100 covered originations in 2025, it will not be a covered financial institution and will not be required to collect data or otherwise comply with the final rule for 2027. However, it must determine if it is required to collect data and otherwise comply for later years.

CONSUMER FINANCIAL PROTECTION BUREAU | MARCH 2023

Supervisory Highlights Junk Fees Special Edition

Issue 29, Winter 2023

cfpb Consumer Financial Protection Bureau

Table of contents

1. Introduction

This special edition of *Supervisory Highlights* focuses on the Consumer Financial Protection Bureau's (CFPB or Bureau) recent supervisory work related to violations of law in connection with fees.[1] As part of its emphasis on fair competition the CFPB has launched an initiative, consistent with its legal authority, to scrutinize exploitative fees charged by banks and financial companies, commonly referred to as "junk fees."

Junk fees are unnecessary charges that inflate costs while adding little to no value to the consumer. Theses unavoidable or surprise charges are often hidden or disclosed only at a later stage in the consumer's purchasing process or sometimes not at all.

The CFPB administers several laws and regulations that may touch on fees including, but not limited to, the Credit Card, Accountability, Responsibility and Disclosure Act of 2009 (CARD Act),[2] the Fair Debt Collection Practices Act (FDCPA),[3] Regulation Z,[4] and the prohibition against unfair, deceptive, or abusive acts or practices (UDAAP) under the Consumer Financial Protection Act of 2010 (CFPA).[5]

The findings in this report cover examinations involving fees in the areas of deposits, auto servicing, mortgage servicing, payday and small dollar lending, and student loan servicing completed between July 1, 2022, and February 1, 2023. To maintain the anonymity of the supervised institutions discussed in *Supervisory Highlights*, references to institutions generally are in the plural and the related findings may pertain to one or more institutions.

We invite readers with questions or comments about *Supervisory Highlights* to contact us at CFPB_Supervision@cfpb.gov.

[1] If a supervisory matter is referred to the Office of Enforcement, Enforcement may cite additional violations based on these facts or uncover additional information that could impact the conclusion as to what violations may exist.
[2] 12 C.F.R. § 1026.
[3] 15 U.S.C. § 1692.
[4] 12 C.F.R. § 1026.
[5] 12 U.S.C. §§ 5531, 5536.

2. Supervisory Observations

2.1 Deposits

During examinations of insured depository institutions and credit unions, Bureau examiners assessed activities related to the imposition of certain fees by the institutions. This included assessing whether entities had engaged in any UDAAPs prohibited by the CFPA.[6]

2.1.1 Unfair Authorize Positive, Settle Negative Overdraft Fees

As described below, Supervision has cited institutions for unfair unanticipated overdraft fees for transactions that authorized against a positive balance, but settled against a negative balance (i.e., APSN overdraft fees). They can occur when financial institutions assess overdraft fees for debit card or ATM transactions where the consumer had a sufficient available balance at the time the financial institution authorized the transaction, but given the delay between authorization and settlement of the transaction the consumer's account balance is insufficient at the time of settlement. This can occur due to intervening authorizations resulting in holds, settlement of other transactions, timing of presentment of the transaction for settlement, and other complex processes relating to transaction order processing practices and other financial institution policies. The Bureau previously discussed this practice in Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices ("Overdraft Circular").[7]

Supervision has cited unfair acts or practices at institutions that charged consumers APSN overdraft fees. An act or practice is unfair when: (1) it causes or is likely to cause substantial injury to consumers; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or to competition.[8]

While work is ongoing, at this early stage, Supervision has already identified at least tens of millions of dollars of consumer injury and in response to these examination findings,

---

[6] 12 U.S.C. §§ 5531, 5536.

[7] Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices (Oct. 26, 2022)("Overdraft Circular"), at 8-12, available at: https://files.consumerfinance.gov/f/documents/cfpb_unanticipated-overdraft-fee-assessment-practices_circular_2022-10.pdf.

[8] 12 U.S.C. § 5531(c).

institutions are providing redress to over 170,000 consumers. Supervision found instances in which institutions assessed unfair APSN overdraft fees using the consumer's available balance for fee decisioning, as well as unfair APSN overdraft fees using the consumer's ledger balance for fee decisioning. Consumers could not reasonably avoid the substantial injury, irrespective of account-opening disclosures. As a result of examiner findings, the institutions were directed to cease charging APSN overdraft fees and to conduct lookbacks and issue remediation to consumers who were assessed these fees.

Supervision also issued matters requiring attention to correct problems that occurred when institutions had enacted policies intended to eliminate APSN overdraft fees, but APSN fees were still charged. Specifically, institutions attempted to prevent APSN overdraft fees by not assessing overdraft fees on transactions which authorized positive, as long as the initial authorization hold was still in effect at or shortly before the time of settlement. There were some transactions, however, that settled outside this time period. Examiners found evidence of inadequate compliance management systems where institutions failed to maintain records of transactions sufficient to ensure overdraft fees would not be assessed, or failed to use some other solution to not charge APSN overdraft fees. In response to these findings, the institutions agreed to implement more effective solutions to avoid charging APSN overdraft fees and to issue remediation to the affected consumers.

The Bureau has stated the legal violations surrounding APSN overdraft fees both generally and in the context of specific public enforcement actions will result in hundreds of millions of dollars of redress to consumers.[9] As discussed in a June 16, 2022 blog post, Supervision has also engaged in a pilot program to collect detailed information about institutions' overdraft practices, including whether institutions charged APSN overdraft fees.[10] A number of banks that had previously reported to Supervision engaging in APSN overdraft fee practices now report that they will stop doing so. Institutions that have reported finalized remediation plans to Supervision state their plans cover time periods starting in 2018 or 2019 up to the point they ceased charging APSN overdraft fees.

---

[9] See Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices (Oct. 26, 2022) available at: https://files.consumerfinance.gov/f/documents/cfpb_unanticipated-overdraft-fee-assessment-practices_circular_2022-10.pdf; CFPB Consent Order 2022-CFPB-008, In the Matter of Regions Bank (Sept. 28, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_Regions_Bank-_Consent-Order_2022-09.pdf; CFPB Consent Order 2022-CFPB-0011, In the Matter of Wells Fargo Bank, (Dec. 20, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

[10] Measuring the impact of financial institution overdraft programs on consumers, (June 16, 2022), available at: https://www.consumerfinance.gov/about-us/blog/measuring-the-impact-of-financial-institution-overdraft-programs-on-consumers/.

2.1.2 Assessing multiple NSF fees for the same transaction

Supervision conducted examinations of institutions to review certain practices related to charging consumers non-sufficient funds (NSF) fees. As described in more detail below, examiners conducted a fact-intensive analysis at various institutions to assess specific types of NSF fees. In some of these examinations, examiners found unfair practices related to the assessment of multiple NSF fees for a single transaction.

Some institutions assess NSF fees when a consumer pays for a transaction with a check or an Automated Clearing House (ACH) transfer and the transaction is presented for payment, but there is not a sufficient balance in the consumer's account to cover the transaction. After declining to pay a transaction, the consumer's account-holding institution will return the transaction to the payee's depository institution due to non-sufficient funds and may assess an NSF fee. The payee may then present the same transaction to the consumer's account-holding institution again for payment. If the consumer's account balance is again insufficient to pay for the transaction, then the consumer's account-holding institution may assess another NSF fee for the transaction and again return the transaction to the payee. Absent restrictions on assessment of NSF fees by the consumer's account-holding institution, this cycle can occur multiple times.

Supervision found that institutions engaged in unfair acts or practices by charging consumers multiple NSF fees when the same transaction was presented multiple times for payment against an insufficient balance in the consumer's accounts, potentially as soon as the next day. The assessment of multiple NSF fees for the same transaction caused substantial monetary harm to consumers, totaling millions of dollars. These injuries were not reasonably avoidable by consumers, regardless of account opening disclosures. And the injuries were not outweighed by countervailing benefits to consumers or competition.

Examiners found that institutions charged several million dollars to tens of thousands of consumers over the course of several years due to their assessment of multiple NSF fees for the same transaction. The institutions agreed to cease charging NSF fees for unpaid transactions entirely and Supervision directed the institutions to refund consumers appropriately. Other regulators have spoken about this practice as well.[11]

In the course of obtaining information about institutions' overdraft and NSF fee practices, examiners obtained information regarding limitations related to the assessment of NSF fees. Supervision subsequently heard from a number of institutions regarding changes to their NSF

[11] NYDFS, Industry Letter: Avoiding Improper Practices Related to Overdraft and Non-Sufficient Funds Fees (July 12, 2022), available at: https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220712_overdraft_nsf_fees; FDIC, Supervisory Guidance on Multiple Re-Presentment NSF Fees (Aug. 2022), available at: https://www.fdic.gov/news/financial-institution-letters/2022/fil22040a.pdf.

fee assessment practices. Virtually all institutions that Supervision has engaged with on this issue reported plans to stop charging NSF fees altogether.

Supervision anticipates engaging in further follow-up work on both multiple NSF fee and APSN overdraft fee issues. In line with the Bureau's statement regarding responsible business conduct, institutions are encouraged to "self-assess [their] compliance with Federal consumer financial law, self-report to the Bureau when [they identify] likely violations, remediate the harm resulting from these likely violations, and cooperate above and beyond what is required by law" with these efforts.[12] As the statement notes, "...the Bureau's Division of Supervision, Enforcement, and Fair Lending makes determinations of whether violations should be resolved through non-public supervisory action or a possible public enforcement action through its Action Review Committee (ARC) process." For those institutions that meaningfully engage in responsible conduct, this "could result in resolving violations non-publicly through the supervisory process."

2.2 Auto Servicing

During auto servicing examinations, examiners identified UDAAPs related to junk fees, such as unauthorized late fees and estimated repossession fees.[13] Additionally, examiners found that servicers charged unfair and abusive payment fees.

2.2.1 Overcharging late fees

Examiners found that servicers engaged in unfair acts or practice by assessing late fees in excess of the amounts allowed by consumers' contracts. Auto contracts often contain language that caps the maximum late fee amounts servicers are permitted to assess. The servicers coded their systems to assess a $25 late fee even though some consumers' loan notes capped late fees at no more than 5% of the monthly payment amount. The $25 late fee exceeded 5% of many consumers' monthly payment amounts. Excessive late fees cost consumers money and thus constitute substantial injury. Consumers could not reasonably avoid the injury because they do not control how servicers calculate late fees, had no reason to anticipate that the servicers would impose excessive late fees, and could not practically avoid being charged a fee. And the injury to consumers was not outweighed by benefits to consumers or competition.

[12] CFPB Bulletin 2020-01, Responsible Business Conduct: Self-Assessing, Self-Reporting, Remediating, and Cooperating, (Mar. 6, 2020), available at: https://files.consumerfinance.gov/f/documents/cfpb_bulletin-2020-01_responsible-business-conduct.pdf.

[13] Note that while involuntary fees are often unfair when they are not authorized by a consumer contract, fees that are disclosed in the contract can also be unfair, depending on the circumstances.

In response to these findings, the servicers ceased the practice and refunded late fee overcharges to consumers.

2.2.2 Charging unauthorized late fees after repossession and acceleration

Examiners found that servicers engaged in unfair acts or practices by assessing late fees not allowed by consumers' contracts. Specifically, the contracts authorized the servicers to charge late fees if consumers' periodic payments were more than 10 days delinquent. But, under the terms of the relevant loan agreements, after the servicers accelerated the loan balance, the entire remaining loan balance became immediately due and payable, thus terminating consumers' contractual obligation to make further periodic payments and eliminating the servicers' contractual right to charge late fees on such periodic payments. Despite this, the servicers continued to collect late fees even after they repossessed the vehicles on periodic payments scheduled to occur subsequent to the date on which the loan balances were accelerated. When consumers redeemed their vehicles by paying the full balance, they also paid these unauthorized late fees; these unauthorized fees caused substantial injury to consumers. Consumers could not reasonably avoid the late fees because they had no control over the servicers' late fee practices. And the injury to consumers was not outweighed by benefits to consumers or competition.

In response to these findings, servicers ceased the practice and refunded late fees to consumers.

2.2.3 Charging estimated repossession fees significantly higher than average repossession costs

Examiners found that, where servicers allowed consumers to recover their vehicles after repossession by paying off the loan balance or past due amounts, servicers charged a $1,000 estimated repossession fee as part of the amount owed. This estimated repossession fee was significantly higher than the average repossession cost, which is generally around $350. By policy, the servicers returned the excess amounts to the consumer after they received the invoice for the actual cost from the repossession agent.

Examiners found that the servicers engaged in unfair acts or practices when they charged estimated repossession fees that were significantly higher than the costs they purported to cover. The relevant contracts permitted the servicers to charge consumers default-related fees based on actual cost, but here the fees significantly exceeded the actual cost. Charging the fees caused or was likely to cause substantial injury in the form of concrete monetary harm. For consumers who paid the amount demanded, deprivation of these funds for even a short period constituted substantial injury. Furthermore, some consumers may have been dissuaded from

recovering their vehicles because the servicers represented that consumers must pay a $1,000 estimated repossession fee in addition to other amounts due. Some consumers may have been able to afford a $350 fee but not a $1,000 fee, and therefore did not pay and permanently lost access to their vehicles. Consumers could not reasonably avoid the injury because they did not control the servicers' practice of charging unauthorized estimated repossession fees. And the injury was not outweighed by countervailing benefits to consumers or competition because the fee exceeded costs necessary to cover repossession.

In response to these findings, the servicers ceased the practice of charging estimated repossession fees that were significantly higher than the actual average amount and provided refunds to affected consumers.

2.2.4 Unfair and abusive payment fees

An act or practice is abusive if it "takes unreasonable advantage of … the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service."[14]

Examiners found that servicers engaged in unfair and abusive acts or practices by charging and profiting from payment processing fees that far exceeded the servicers' costs for processing payments, after the consumer was locked into a relationship with a servicer chosen by the dealer. Examiners observed that the servicers only offered two free payment options—pre-authorized recurring ACH and mailed checks—which are only available to consumers with bank accounts. Approximately 90 percent of payments made by consumers incurred a pay-to-pay fee. The servicers received over half the amount of these fees from the servicers' third-party payment processor as incentive payments, totaling millions of dollars.

Examiners concluded that these practices took unreasonable advantage of consumers' inability to protect their interests by charging consumers fees to use the most common payment methods to pay their auto loans, after the consumer was locked into a relationship with a servicer, that far exceeded the servicers' costs. Servicers leveraged their captive customer base and profited off payment fees through kickback incentive payments. These consumers were unable to protect their interests in selecting or using a consumer financial product or service because the dealer, not the consumer, selected the servicer. Consumers thus could not evaluate a servicer's payment processing fees, bargain over these fees, or switch to a servicer with lower-cost or more no-fee payment options.

[14] 12 U.S.C. § 5531(d)(2)(B).

In addition, examiners found that these practices were unfair. The payment processing fees constituted substantial injury. Because consumers did not choose their auto loan servicers, they could not reasonably avoid these costs by bargaining with the servicer over the fees or switching to another servicer; moreover, consumers without bank accounts, who were unaware of the payment structure, or who have other obstacles to ACH or check payments, could not use the free payment methods and thus could not reasonably avoid paying the fees. And the injury to consumers was not outweighed by benefits to consumers or competition.

In response to these findings, Supervision directed the servicers to cease the practice.

2.3 Mortgage Servicing

In conducting mortgage servicing examinations, examiners identified a number of UDAAPs and a Regulation Z violation related to junk fees. Examiners found that servicers charged consumers junk fees that were unlawful related to late fee amounts, unnecessary property inspection visits, and private mortgage insurance (PMI) charges that should have been billed to the lender. Servicers also failed to waive certain charges when consumers entered permanent loss mitigation options and failed to refund PMI premiums. And servicers charged consumers late fees after sending periodic statements representing that they would not charge late fees.

2.3.1 Overcharging late fees

Examiners found that servicers engaged in unfair acts or practices by assessing late fees in excess of the amounts allowed by their loan agreements. Specifically, where loan agreements included a maximum permitted late fee amount, the servicers failed to input these late fee caps into their systems. Because the systems did not reflect the maximum late fee amounts permitted by their loan agreements, the servicers charged the maximum allowable late fees under the relevant state laws, which frequently exceeded the specific caps in the loan agreements. The servicers caused substantial injury to consumers when they imposed these excessive late fees. Consumers could not reasonably avoid the injury because they do not control how servicers calculate late fees and had no reason to anticipate that servicers would impose excessive late fees. Charging excessive late fees had no benefits to consumers or competition. Examiners concluded that servicers also violated Regulation Z[15] by issuing periodic statements that included inaccurate late payment fee amounts, since they exceeded the

[15] 12 C.F.R. § 1026.41(d)(1)(ii).

amounts allowed by the loan agreements. In response to these findings, servicers waived or refunded late fee overcharges to consumers and corrected the periodic statements.

2.3.2 Repeatedly charging consumers for unnecessary property inspections

Mortgage investors generally require servicers to perform property inspection visits for accounts that reach a specified level of delinquency. Generally, servicers must complete these property inspections monthly. To satisfy this requirement, servicers hire a third party that sends an agent to physically locate and view the property. The servicers then pass along the cost of the property inspection to the consumer, with fees ranging from $10 to $50.

Examiners found that in some instances a property inspector would report to servicers that an address was incorrect, and that the inspectors could not locate the property because of this error. Despite knowing that the address was incorrect, the servicers repeatedly hired property inspectors to visit these properties. Examiners found that servicers engaged in an unfair act or practice when they charged consumers for repeat property preservation visits to known bad addresses. Charging consumers for property inspection fees to known bad addresses caused consumers substantial injury. Consumers were unable to anticipate the fees or mitigate them because they have no influence over the servicers' practices, and the servicers did not inform consumers that they had bad addresses. And the injury caused by the practice was not outweighed by countervailing benefits to consumers or competition.

In response to the findings, the servicers revised their policies and procedures and waived or refunded the fees.

2.3.3 Misrepresenting that consumers owed PMI premiums

Examiners found that servicers engaged in deceptive acts or practices by sending monthly periodic statements and escrow disclosures that included monthly private mortgage insurance (PMI) premiums that consumers did not owe. These consumers did not have borrower-paid PMI on their accounts; instead, the loans were originated with lender-paid PMI, which should not be billed directly to consumers. After receiving these statements and disclosures some consumers made overpayments that included these amounts.

A representation, omission, act, or practice is deceptive when: (1) The representation, omission, act, or practice misleads or is likely to mislead the consumer; (2) The consumer's interpretation of the representation, omission, act, or practice is reasonable under the circumstances; and

(3) the misleading representation, omission, act, or practice is material.[16] The servicers' statements were likely to mislead consumers by creating the false impression that PMI payments were due. It was reasonable for consumers to rely on the servicers' calculations to determine the appropriate monthly payment amount. Finally, the misrepresentations were material because they led to overpayments. In response to these findings, the servicers refunded any overpayments.

2.3.4 Charging consumers fees that should have been waived

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) directs servicers of federally backed mortgages to grant consumers a forbearance from monthly mortgage payments if the consumer is experiencing a financial hardship as a result of the COVID-19 emergency. During the time a consumer is in forbearance, no fees, penalties, or additional interest beyond scheduled amounts are to be assessed. While the CARES Act prohibits fees, penalties, or additional interest beyond scheduled amounts during a forbearance period, consumers sometimes accrue these amounts during periods when they are not in forbearance. For example, a servicer could appropriately charge a late fee if a consumer was delinquent in May 2020 and then entered a forbearance in June 2020.

When consumers with Federal Housing Administration-insured loans exited CARES Act forbearances and entered certain permanent loss mitigation options, the Department of Housing and Urban Development (HUD) required servicers in certain circumstances to waive late charges, fees, and penalties accrued outside of forbearance periods.

Examiners found that servicers engaged in unfair acts or practices when they failed to waive certain late charges, fees, and penalties accrued outside forbearance periods, where required by HUD, upon a consumer entering a permanent COVID-19 loss mitigation option.[17] Failure to waive the late charges, fees, and penalties constituted substantial injury to consumers. This injury was not reasonably avoidable by consumers because they had no reason to anticipate that their servicer would fail to follow HUD requirements, and consumers lacked reasonable means to avoid the charges. This harm outweighed any benefit to consumers or competition. In response to the finding, the servicers improved their controls, waived all improper charges, and provided refunds to consumers.

[16] 12 U.S.C. §§ 5531 and 5536(a)(1)(B).
[17] The Bureau previously reported a different unfair act or practice of charging fees to consumers during a CARES Act forbearance in Supervisory Highlights, Issue 25, Fall 2021, available at: https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-25_2021-12.pdf.

2.3.5 Charging consumers for PMI after it should have been removed

The Homeowners Protection Act (HPA) requires that servicers automatically terminate PMI when the principal balance of the mortgage loan is first scheduled to reach 78 percent of the original value of the property based on the applicable amortization schedule, as long as the borrower is current.[18] Examiners found that servicers violated the HPA when they failed to terminate PMI on the date the principal balance of the mortgage was first scheduled to reach 78 percent loan-to-value on a mortgage loan that was current. As a result, consumers made overpayments for PMI that the servicers should have cancelled. In response to these findings, the servicers refunded excess PMI payments and implemented additional procedures and controls to enhance their PMI handling.[19]

2.3.6 Charging late fees after sending periodic statements listing a $0 late fee

Examiners found that servicers sent periodic statements to consumers in their last month of forbearance that incorrectly listed a $0 late fee amount for the subsequent payment, when a late fee was in fact charged if a payment was late. For example, consumers whose loans were in a forbearance period that ended on October 31st received a periodic statement during October billing for the November 1st payment; the periodic statement listed a $0 late fee amount. But because the November 1st payment was due after the forbearance period ended, the servicers then charged these consumers their contractual late fee amount if they missed the November 1st payment, despite sending statements listing a $0 late fee.

Examiners found that this practice was deceptive. Consumers' interpretation that they would incur no late fee was reasonable under the circumstances; consumers reasonably assume that the payment amounts and fees servicers tell them to pay are accurate and truthful. And the misrepresentations were likely to be material because consumers may have elected to make a timely periodic payment if the servicers had accurately advised a late fee would be assessed.

In response to this finding, the servicers updated their periodic statements and waived or refunded late fee charges for the specific payments.

[18] 12 U.S.C. § 4902(b)(1).
[19] The Bureau previously reported similar violations in Supervisory Highlights, Issue 25, Fall 2021, available at: https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-25_2021-12.pdf.

2.4 Payday and Small-Dollar Lending

2.4.1 Splitting and re-presenting consumer payments without authorization

Examiners found that lenders, in connection with payday, installment, title, and line-of-credit loans, after unsuccessful debit attempts, split missed payments into as many as four sub-payments and simultaneously or near-simultaneously represented them to consumers' banks for payment via debit card.

Examiners found that lenders engaged in unfair acts or practices when they re-presented split payments from consumers' accounts without their authorization to do so simultaneously or near-simultaneously. As a consequence, consumers incurred or were likely to incur injury in the form of multiple overdraft fees, indirect follow-on fees, unauthorized loss of funds, and inability to prioritize payment decisions. Injury was not reasonably avoidable because lenders did not disclose, and consumers had not authorized, same-day, simultaneous or near-simultaneous split debit processing. Substantial injuries were not outweighed by countervailing benefits to consumers or to competition.

In response to these findings, lenders were directed to: (1) provide remediation; (2) stop engaging in split-debit or other payment re-presentment attempts following an initial failed debit attempt, without first obtaining the consumer's authorization as to the manner and timing of the re-presentments; and (3) stop the practice of splitting the single amount owed into several debit attempts, unless the consumer has sufficient time between each debit attempt to learn of any successful debits and to take action to avoid incurring unwanted consequences, such as bank overdraft fees, indirect follow-on fees, unauthorized loss of funds, or inability to prioritize payment decisions.

2.4.2 Charging borrowers repossession-related fees not authorized in automobile title loan contracts

Examiners found that lenders engaged in unfair acts or practices when they charged borrowers fees to retrieve personal property from repossessed vehicles and to cover servicer charges, and withheld the personal property and vehicles until borrowers paid the fees. The practices caused or were likely to cause substantial injury when lenders, through their repossession agents, withheld personal property and vehicles until consumers paid unexpected personal property retrieval fees and agent fees for vehicle redemption. In addition to being subject to unexpected fees, borrowers faced being denied access to or destruction of property such as medical

equipment and vehicles necessary for basic life functions. Potential countervailing benefits to consumers or to competition did not outweigh the substantial injuries caused.

Lenders were directed to enhance their compliance management systems to prevent these practices and to provide remediation to affected consumers.

2.4.3 Failure to timely stop repossessions, charging fees and refinancing despite prior payment arrangements

Examiners found that lenders engaged in unfair acts or practices by failing to stop vehicle repossessions before title loan payments were due as-agreed, and then withholding the vehicles until consumers paid repossession-related fees and refinanced their debts. The practice caused or was likely to cause substantial injury by depriving consumers of their means of transportation and of the contents of their vehicles including medication, by causing them to spend time reclaiming the vehicles, and by imposing repossession fees and refinancing costs. Consumers had no way to stop lenders from disregarding payment agreements specifically designed to prevent repossession. Therefore, they could not reasonably anticipate or avoid the injuries caused. Countervailing benefits of the practice, such as the cost of implementing controls to prevent wrongful repossessions, did not outweigh the substantial injury caused.

Lenders were directed to enhance their compliance management systems to prevent these practices and to provide remediation to affected consumers.

2.5 Student Loan Servicing

2.5.1 Charging late fees and interest after reversing payments

Examiners found that servicers engaged in unfair acts or practices by initially processing payments but then later reversing those payments, leading to additional late fees and interest for consumers. Although the servicers' policies did not allow student loan payments to be made with a credit card, customer service representatives erroneously accepted credit card payment information from some consumers over the phone and then processed those credit card payments. Subsequently, the servicers manually reversed the payments because they violated their policies. As a result, consumers became delinquent on their accounts and suffered substantial injury in the form of late fees, negative credit reporting, and additional accrued interest. Consumers could not reasonably avoid the injury because they could not anticipate that servicers would reverse payments after initially accepting them, and the servicers did not

send notices explaining the reversals in all cases. Moreover, the servicers did not provide consumers with an opportunity to make a payment with another method before reversing the payments. Finally, retroactively reversing credit card payments, as opposed to implementing measures to prevent such payments in the first instance, has no benefits to consumers or to competition.

In response to these findings, the servicers enhanced controls to ensure that payment processing systems will not accept credit card payments and to train customer service representatives to inform consumers at the time of payment that credit cards are not accepted. Additionally, Supervision directed the servicers to reimburse any late fees and correct any negative credit reporting as a result of reversed credit card payments.

3. Supervisory Program Developments

3.1 Recent Bureau Supervisory Program Developments

Set forth below are CFPB-issued circulars, bulletins, advisory opinions, and proposed rules regarding fees.[20]

3.1.1 CFPB proposed a rule to curb excessive credit card late fees

On February 1, 2023, the CFPB proposed a rule to curb excessive credit card late fees that cost American families about $12 billion each year.[21] The CFPB's proposed rule would amend regulations implementing the CARD Act to ensure that late fees meet the Act's requirement to be "reasonable and proportional" to the costs incurred by issuers to handle late payments. Specifically, the proposed rule would lower the immunity provision for late fees to $8 for a missed payment and end the automatic annual inflation adjustment. The proposed rule would also ban late fee amounts above 25% of the consumer's required payment.

3.1.2 CFPB issued circular on unanticipated overdraft fee assessment practices

On October 26, 2022, the CFPB issued guidance indicating that overdraft fees may constitute an unfair act or practice under the CFPA, even if the entity complies with the Truth in Lending Act (TILA) and Regulation Z, and the Electronic Fund Transfer Act (EFTA) and Regulation E.[22] As detailed in the circular, when financial institutions charge surprise overdraft fees, sometimes as much as $36, they may be breaking the law. The circular provides some examples of potentially unlawful surprise overdraft fees, including charging fees on purchases made with a positive

---

[20] Some of these items were also referenced in the last edition of *Supervisory Highlights*.

[21] The proposed rule is available at: https://www.consumerfinance.gov/rules-policy/notice-opportunities-comment/credit-card-penalty-fees-regulation-z/.

[22] Consumer Financial Protection Circular 2022-06, Unanticipated Overdraft Fee Assessment Practices (Oct. 26, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_unanticipated-overdraft-fee-assessment-practices_circular_2022-10.pdf.

balance. These overdraft fees occur when a bank displays that a customer has sufficient available funds to complete a debit card purchase at the time of the transaction, but the consumer is later charged an overdraft fee. Often, the financial institution relies on complex back-office practices to justify charging the fee. For instance, after the bank allows one debit card transaction when there is sufficient money in the account, it nonetheless charges a fee on that transaction later because of intervening transactions.

3.1.3 CFPB issued bulletin on unfair returned deposited item fee assessment practices

On October 26, 2022, the CFPB issued a bulletin[23] stating that blanket policies of charging returned deposited item fees to consumers for all returned transactions irrespective of the circumstances or patterns of behavior on the account are likely unfair under the CFPA.

3.1.4 CFPB issued advisory opinion on debt collectors' collection of pay-to-pay fees

On June 29, 2022, the CFPB issued an advisory opinion[24] affirming that federal law often prohibits debt collectors from charging "pay-to-pay" fees. These charges, commonly described by debt collectors as "convenience fees," are imposed on consumers who want to make a payment in a particular way, such as online or by phone.

[23] Bulletin 2022-06: Unfair Returned Deposited Item Fee Assessment Practices, available at: https://files.consumerfinance.gov/f/documents/cfpb_returned-deposited-item-fee-assessment-practice_compliance-bulletin_2022-10.pdf.

[24] Advisory Opinion on Debt Collectors' Collection of Pay-to-Pay Fees, available at: https://files.consumerfinance.gov/f/documents/cfpb_convenience-fees_advisory-opinion_2022-06.pdf.

4. Remedial Actions

4.1 Public Enforcement Actions

The Bureau's supervisory activities resulted in and supported the following enforcement actions.

4.1.1 Wells Fargo

On December 20, 2022, the CFPB and Wells Fargo entered into a consent order in which Wells Fargo will pay more than $2 billion in redress to consumers and a $1.7 billion civil penalty for legal violations across several of its largest product lines.[25] The bank's illegal conduct led to billions of dollars in financial harm to its customers and, for thousands of customers, the loss of their vehicles and homes. Consumers were illegally assessed fees and interest charges on auto and mortgage loans, had their cars wrongly repossessed, and had payments to auto and mortgage loans misapplied by the bank. Wells Fargo also improperly froze or closed customer deposit accounts, charged consumers unlawful surprise overdraft fees, and did not always waive monthly account service fees consistent with its disclosures. Under the terms of the order, Wells Fargo will pay redress to the over 16 million affected consumer accounts, and pay a $1.7 billion fine, which will go to the CFPB's Civil Penalty Fund, where it will be used to provide relief to victims of consumer financial law violations.

4.1.2 Regions Bank

On September 28, 2022, the CFPB ordered Regions Bank to pay $50 million into the CFPB's victims relief fund and to refund at least $141 million to customers harmed by its illegal surprise overdraft fees.[26] Until July 2021, Regions charged customers surprise overdraft fees on certain ATM withdrawals and debit card purchases. The bank charged overdraft fees even after telling consumers they had sufficient funds at the time of the transactions. The CFPB also found that Regions Bank leadership knew about and could have discontinued its surprise overdraft fee practices years earlier, but they chose to wait while Regions pursued changes that would generate new fee revenue to make up for ending the illegal fees.

---

[25] CFPB Consent Order 2022-CFPB-0011, In the Matter of Wells Fargo Bank (Dec. 20, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_wells-fargo-na-2022_consent-order_2022-12.pdf.

[26] CFPB Consent Order 2022-CFPB-0008, In the Matter of Regions Bank (Sept. 28, 2022), available at: https://files.consumerfinance.gov/f/documents/cfpb_Regions_Bank-_Consent-Order_2022-09.pdf.

This is not the first time Regions Bank has been caught engaging in illegal overdraft abuses. In 2015, the CFPB found that Regions had charged $49 million in unlawful overdraft fees and ordered Regions to make sure that the fees had been fully refunded and pay a $7.5 million penalty for charging overdraft fees to consumers who had not opted into overdraft protection and to consumers who had been told they would not be charged overdraft fees.[27]

[27] CFPB Consent Order 2015, In the Matter of Regions Bank, (Apr. 28, 2015), available at: https://files.consumerfinance.gov/f/201504_cfpb_consent-order_regions-bank.pdf.

PART 1001—FINANCIAL PRODUCTS OR SERVICES

1. The authority citation for part 1001 continues to read as follows:

AUTHORITY: 12 U.S.C. 5481(15)(A)(xi); and 12 U.S.C. 5512(b)(1).

2. Section 1001.2 is amended by revising paragraph (b) and by adding and reserving paragraph (c) to read as follows:

§ 1001.2 Definitions.* * * * *

(b) Providing financial data processing products or services by any technological means, including processing, storing, aggregating, or transmitting financial or banking data, alone or in connection with another product or service, where the financial data processing is not offered or provided by a person who, by operation of 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person.

(c) [Reserved].

3. Part 1033 is added to read as follows:

PART 1033—PERSONAL FINANCIAL DATA RIGHTS

SUBPART A—GENERAL

Sec.

SUBPART B—OBLIGATION TO MAKE COVERED DATA AVAILABLE

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

SUBPART D—AUTHORIZED THIRD PARTIES

AUTHORITY: 12 U.S.C. 5512; 12 U.S.C. 5514; 12 U.S.C. 5532; 12 U.S.C. 5533.

SUBPART A—GENERAL

§ 1033.101 Authority, purpose, and organization.

(a) *Authority*. The regulation in this part is issued by the Consumer Financial Protection Bureau (CFPB) pursuant to the Consumer Financial Protection Act of 2010 (CFPA), Pub. L. 111-203, tit. X, 124 Stat. 1955.

(b) *Purpose*. This part implements the provisions of section 1033 of the CFPA by requiring data providers to make available to consumers and authorized third parties, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service, in an electronic form usable by consumers and authorized third parties; and by prescribing standards to promote the development and use of standardized formats for covered data, including through industry standards developed by standard-setting bodies recognized by the CFPB. This part also sets forth obligations of third parties that would access covered data on a consumer's behalf, including limitations on their collection, use, and retention of covered data.

(c) *Organization*. This part is divided into subparts as follows:

(1) Subpart A establishes the authority, purpose, organization, coverage of data providers, compliance dates, and definitions applicable to this part.

(2) Subpart B provides the general obligation of data providers to make covered data available upon the request of a consumer or authorized third party, including what types of information must be made available.

(3) Subpart C provides the requirements for data providers to establish and maintain interfaces to receive and respond to requests for covered data.

(4) Subpart D provides the obligations of third parties that would access covered data on behalf of a consumer.

§ 1033.111 Coverage of data providers.

(a) *Coverage of data providers.* A data provider has obligations under this part if it controls or possesses covered data concerning a covered consumer financial product or service, subject to the exclusion in paragraph (d) of this section.

(b) *Definition of covered consumer financial product or service*. *Covered consumer financial product or service* means a consumer financial product or service, as defined in 12 U.S.C. 5481(5), that is:

(1) A *Regulation E account*, which means an account, as defined in Regulation E, 12 CFR 1005.2(b);

(2) A *Regulation Z credit card*, which means a credit card, as defined in Regulation Z, 12 CFR 1026.2(a)(15)(i); and

(3) Facilitation of payments from a Regulation E account or Regulation Z credit card.

(c) *Definition of data provider*. *Data provider* means a covered person, as defined in 12 U.S.C. 5481(6), that is:

(1) A *financial institution*, as defined in Regulation E, 12 CFR 1005.2(i);

(2) A *card issuer*, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or

(3) Any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person.

Example 1 to paragraph (c): A digital wallet provider is a data provider.

(d) *Excluded data providers*. The requirements of this part do not apply to data providers that are depository institutions that do not have a consumer interface.

§ 1033.121 Compliance dates.

A data provider must comply with §§ 1033.201 and 1033.301 beginning on:

(a) [Approximately six months after the date of publication of the final rule in the *Federal Register*], for depository institution data providers that hold at least $500 billion in total assets and nondepository institution data providers that generated at least $10 billion in revenue in the preceding calendar year or are projected to generate at least $10 billion in revenue in the current calendar year.

(b) [Approximately one year after the date of publication of the final rule in the *Federal Register*], for data providers that are:

(1) Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets; or

(2) Nondepository institutions that generated less than $10 billion in revenue in the preceding calendar year and are projected to generate less than $10 billion in revenue in the current calendar year.

(c) [Approximately two and a half years after the date of publication of the final rule in the *Federal Register*], for depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.

(d) [Approximately four years after the date of publication of the final rule in the *Federal Register*], for depository institutions that hold less than $850 million in total assets.

§ 1033.131 Definitions.

For purposes of this part, the following definitions apply:

Authorized third party means a third party that has complied with the authorization procedures described in § 1033.401.

Card issuer is defined at § 1033.111(c)(2).

Consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of this definition.

Consumer interface means an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by consumers in response to the requests.

Covered consumer financial product or service is defined at § 1033.111(b).

Covered data is defined at § 1033.211.

Data aggregator means an entity that is retained by and provides services to the authorized third party to enable access to covered data.

Data provider is defined at § 1033.111(c).

Developer interface means an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by authorized third parties in response to the requests.

Financial institution is defined at § 1033.111(c)(1).

Qualified industry standard means a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with § 1033.141(a).

Regulation E account is defined at § 1033.111(b)(1).

Regulation Z credit card is defined at § 1033.111(b)(2).

Third party means any person or entity that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data.

§ 1033.141 Standard setting.

(a) *Fair, open, and inclusive standard-setting body*. A standard-setting body is fair, open, and inclusive and is an issuer of qualified industry standards when it has all of the following attributes:

(1) Openness: The sources, procedures, and processes used are open to all interested parties, including: consumer and other public interest groups with expertise in consumer protection, financial services, community development, fair lending, and civil rights; authorized third parties; data providers; data aggregators and other providers of services to authorized third parties; and relevant trade associations. Parties can meaningfully participate in standards development on a non-discriminatory basis.

(2) Balance: The decision-making power is balanced across all interested parties, including consumer and other public interest groups, at all levels of the standard-setting body. There is meaningful representation for large and small commercial entities within these categories. No single interest or set of interests dominates decision-making. Achieving balance requires recognition that some participants may play multiple roles, such as being both a data provider and an authorized third party. The ownership structure of entities is considered in achieving balance.

(3) Due process: The standard-setting body uses documented and publicly available policies and procedures, and it provides adequate notice of meetings and standards development,

sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views.

(4) Appeals: An appeals process is available for the impartial handling of appeals.

(5) Consensus: Standards development proceeds by consensus, which is defined as general agreement, but not unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

(6) Transparency: Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

(7) CFPB recognition: The standard-setting body has been recognized by the CFPB within the last three years as an issuer of qualified industry standards.

(b) *CFPB consideration*. A standard-setting body may request that the CFPB recognize it as an issuer of qualified industry standards. The attributes set forth in paragraphs (a)(1) through (6) of this section will inform the CFPB's consideration of the request.

SUBPART B—OBLIGATION TO MAKE COVERED DATA AVAILABLE

§ 1033.201 Obligation to make covered data available.

(a) *Obligation to make covered data available*. A data provider must make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider, in an electronic form usable by consumers and authorized third parties. Compliance with the requirements in §§ 1033.301 and 1033.311 is required in addition to the requirements of this paragraph (a).

(b) *Current data*. In complying with paragraph (a) of this section, a data provider must make available the most recently updated covered data that it has in its control or possession at

the time of a request. A data provider must make available information concerning authorized but not yet settled debit card transactions.

§ 1033.211 Covered data.

Covered data in this part means, as applicable:

(a) Transaction information, including historical transaction information in the control or possession of the data provider. A data provider is deemed to make available sufficient historical transaction information for purposes of § 1033.201(a) if it makes available at least 24 months of such information.

Example 1 to paragraph (a): This category includes amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges.

(b) Account balance.

(c) Information to initiate payment to or from a Regulation E account.

Example 1 to paragraph (c): This category includes a tokenized account and routing number that can be used to initiate an Automated Clearing House transaction. In complying with its obligation under § 1033.201(a), a data provider is permitted to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number.

(d) Terms and conditions.

Example 1 to paragraph (d): This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.

(e) Upcoming bill information.

Example 1 to paragraph (e): This category includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.

(f) Basic account verification information, which is limited to the name, address, email address, and phone number associated with the covered consumer financial product or service.

§ 1033.221 Exceptions.

A data provider is not required to make available the following covered data to a consumer or authorized third party:

(a) Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. Information does not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor. For example, annual percentage rate and other pricing terms are sometimes determined by an internal algorithm or predictor but do not fall within this exception.

(b) Any information collected by the data provider for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct. Information collected for other purposes does not fall within this exception. For example, name and other basic account verification information do not fall within this exception.

(c) Any information required to be kept confidential by any other provision of law. Information does not qualify for this exception merely because the data provider must protect it for the benefit of the consumer. For example, the data provider cannot restrict access to the consumer's own information merely because that information is subject to privacy protections.

(d) Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

§ 1033.301 General requirements.

(a) *Requirement to establish and maintain interfaces*. A data provider subject to the requirements of this part must maintain a consumer interface and must establish and maintain a

developer interface. The consumer interface and the developer interface must satisfy the requirements set forth in this section. The developer interface must satisfy the additional requirements set forth in § 1033.311.

(b) *Machine-readable files upon specific request*. Upon specific request, a data provider must make available to a consumer or an authorized third party covered data in a machine-readable file that can be retained by the consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.

Example 1 to paragraph (b): A data provider makes available covered data in a machine-readable file that can be retained if the data can be printed or kept in a separate information system that is in the control of the consumer or authorized third party.

(c) *Fees prohibited.* A data provider must not impose any fees or charges on a consumer or an authorized third party in connection with:

(1) *Interfaces*. Establishing or maintaining the interfaces required by paragraph (a) of this section; or

(2) *Requests*. Receiving requests or making available covered data in response to requests as required by this part.

§ 1033.311 Requirements applicable to developer interface.

(a) *General.* A developer interface required by § 1033.301(a) must satisfy the requirements set forth in this section.

(b) *Standardized format*. The developer interface must make available covered data in a standardized format. The interface is deemed to satisfy this requirement if:

(1) The interface makes available covered data in a format that is set forth in a qualified industry standard; or

(2) In the absence of a qualified industry standard, the interface makes available covered data in a format that is widely used by the developer interfaces of other similarly situated data providers with respect to similar data and is readily usable by authorized third parties.

(c) *Performance specifications.* The developer interface must satisfy the following performance specifications:

(1) *Commercially reasonable performance.* The performance of the interface must be commercially reasonable.

(i) *Quantitative minimum performance specification.* The performance of the interface cannot be commercially reasonable if it does not meet the following quantitative minimum performance specification regarding its response rate: The number of proper responses by the interface divided by the total number of queries for covered data to the interface must be equal to or greater than 99.5 percent. For purposes of this paragraph (c)(1)(i), all of the following requirements apply:

(A) Any responses by and queries to the interface during scheduled downtime for the interface must be excluded respectively from the numerator and the denominator of the calculation.

(B) In order for any downtime of the interface to qualify as scheduled downtime, the data provider must have provided reasonable notice of the downtime to all third parties to which the data provider has granted access to the interface. Indicia that the data provider's notice of the downtime may be reasonable include that the notice adheres to a qualified industry standard.

(C) The total amount of scheduled downtime for the interface in the relevant time period, such as a month, must be reasonable. Indicia that the total amount of scheduled downtime may be reasonable include that the amount adheres to a qualified industry standard.

(D) A proper response is a response, other than any message such as an error message provided during unscheduled downtime of the interface, that meets all of the following criteria:

(*1*) The response either fulfills the query or explains why the query was not fulfilled;

(*2*) The response is consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a); and

(*3*) The response is provided by the interface within a commercially reasonable amount of time. The amount of time cannot be commercially reasonable if it is more than 3,500 milliseconds.

(ii) *Indicia of compliance*. Indicia that the performance of the interface is commercially reasonable include that it:

(A) Meets the applicable performance specifications set forth in a qualified industry standard; and

(B) Meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers.

(2) *Access cap prohibition*. Except as otherwise permitted by §§ 1033.221, 1033.321, and 1033.331(b) and (c), a data provider must not unreasonably restrict the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface. Any frequency restrictions must be applied in a manner that is non-discriminatory and consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a). Indicia that any frequency restrictions applied are reasonable include that they adhere to a qualified industry standard.

(d) *Security specifications*—(1) *Access credentials*. A data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface.

(2) *Security program.* (i) A data provider must apply to the developer interface an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or

(ii) If the data provider is not subject to section 501 of the Gramm-Leach-Bliley Act, the data provider must apply to its developer interface the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

§ 1033.321 Interface access.

(a) *Denials related to risk management*. A data provider does not violate the general obligation in § 1033.201(a) by reasonably denying a consumer or third party access to an interface described in § 1033.301(a) based on risk management concerns. Subject to paragraph (b) of this section, a denial is not unreasonable if it is necessary to comply with section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1 or section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801.

(b) *Reasonable denials.* To be reasonable pursuant to paragraph (a) of this section, a denial must, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner.

(c) *Indicia of reasonable denials.* Indicia that a denial pursuant to paragraph (a) of this section is reasonable include whether access is denied to adhere to a qualified industry standard related to data security or risk management.

(d) *Denials related to lack of information.* A data provider has a reasonable basis for denying access to a third party under paragraph (a) of this section if:

(1) The third party does not present evidence that its data security practices are adequate to safeguard the covered data, provided that the denial of access is not otherwise unreasonable; or

(2) The third party does not make the following information available in both human-readable and machine-readable formats, and readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website:

(i) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;

(ii) A link to its website;

(iii) Its Legal Entity Identifier (LEI) that is issued by:

(A) A utility endorsed by the LEI Regulatory Oversight Committee, or

(B) A utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system; and

(iv) Contact information a data provider can use to inquire about the third party's data security practices.

§ 1033.331 Responding to requests for information.

(a) *Responding to requests—access by consumers*. To comply with the requirement in § 1033.201(a), upon request from a consumer, a data provider must make available covered data when it receives information sufficient to:

(1) Authenticate the consumer's identity; and

(2) Identify the scope of the data requested.

(b) *Responding to requests—access by third parties.* (1) To comply with the requirement in § 1033.201(a), upon request from an authorized third party, a data provider must make available covered data when it receives information sufficient to:

(i) Authenticate the consumer's identity;

(ii) Authenticate the third party's identity;

(iii) Confirm the third party has followed the authorization procedures in § 1033.401; and

(iv) Identify the scope of the data requested.

(2) The data provider is permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm:

(i) The account(s) to which the third party is seeking access; and

(ii) The categories of covered data the third party is requesting to access, as disclosed by the third party pursuant to § 1033.411(b)(4).

(c) *Response not required.* Notwithstanding the general rules in paragraphs (a) and (b) of this section, a data provider is not required to make covered data available in response to a request when:

(1) The data are withheld because an exception described in § 1033.221 applies;

(2) The data provider has a basis to deny access pursuant to risk management concerns in accordance with § 1033.321(a);

(3) The data provider's interface is not available when the data provider receives a request requiring a response under this section. However, the data provider is subject to the performance specifications in § 1033.311(c);

(4) The request is for access by a third party, and:

(i) The consumer has revoked the third party's authorization pursuant to paragraph (e) of this section;

(ii) The data provider has received notice that the consumer has revoked the third party's authorization pursuant to § 1033.421(h)(2); or

(iii) The consumer has not provided a new authorization to the third party after the maximum duration period, as described in § 1033.421(b)(2).

(d) *Jointly held accounts.* A data provider that receives a request for covered data from a consumer that jointly holds an account or from an authorized third party acting on behalf of such a consumer must make available covered data to that consumer or authorized third party, subject to the other requirements of this section.

(e) *Mechanism to revoke third party authorization to access covered data.* A data provider does not violate the general obligation in § 1033.201(a) by making available to the consumer a reasonable method to revoke any third party's authorization to access all of the consumer's covered data. To be reasonable, the revocation method must, at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party. Indicia that the data provider's revocation method is reasonable include its conformance to a qualified industry

standard. A data provider that receives a revocation request from consumers through a revocation method it makes available must notify the authorized third party of the request.

§ 1033.341 Information about the data provider.

(a) *Requirement to make information about the data provider readily identifiable*. A data provider must make the information described in paragraphs (b) through (d) of this section:

(1) Readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website; and

(2) Available in both human-readable and machine-readable formats.

(b) *Identifying information*. A data provider must disclose in the manner required by paragraph (a) of this section:

(1) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;

(2) A link to its website;

(3) Its LEI that is issued by:

(i) A utility endorsed by the LEI Regulatory Oversight Committee, or

(ii) A utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system; and

(4) Contact information that enables a consumer or third party to receive answers to questions about accessing covered data under this part.

(c) *Developer interface documentation*. For its developer interface, a data provider must disclose in the manner required by paragraph (a) of this section documentation, including metadata describing all covered data and their corresponding data fields, and other

documentation sufficient for a third party to access and use the interface. The documentation must:

(1) Be maintained and updated as the developer interface is updated;

(2) Include how third parties can get technical support and report issues with the interface; and

(3) Be easy to understand and use, similar to data providers' documentation for other commercially available products.

(d) *Performance specification*. On or before the tenth calendar day of each calendar month, a data provider must disclose in the manner required by paragraph (a) of this section the quantitative minimum performance specification described in § 1033.311(c)(1)(i) that the data provider's developer interface achieved in the previous calendar month. The data provider's disclosure must include at least a rolling 13 months of the required monthly figure, except that the disclosure need not include the monthly figure for months prior to the compliance date applicable to the data provider. The data provider must disclose the metric as a percentage rounded to four decimal places, such as "99.9999 percent."

§ 1033.351 Policies and procedures.

(a) *Reasonable written policies and procedures*. A data provider must establish and maintain written policies and procedures that are reasonably designed to achieve the objectives set forth in subparts B and C of this part, including paragraphs (b) through (d) of this section. Policies and procedures must be appropriate to the size, nature, and complexity of the data provider's activities. A data provider must periodically review the policies and procedures required by this section and update them as appropriate to ensure their continued effectiveness.

(b) *Policies and procedures for making covered data available.* The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that:

(1) *Making available covered data.* A data provider creates a record of the data fields that are covered data in the data provider's control or possession, what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reasons the exception applies. A data provider is permitted to comply with this requirement by incorporating the data fields defined by a qualified industry standard, provided doing so is appropriate to the size, nature, and complexity of the data provider's activities. Exclusive reliance on data fields defined by a qualified industry standard would not be appropriate if such data fields failed to identify all the covered data in the data provider's control or possession.

(2) *Denials of developer interface access.* When a data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider:

(i) Creates a record explaining the basis for denial; and

(ii) Communicates to the third party, electronically or in writing, the reason(s) for the denial, and that the communication occurs as quickly as is practicable.

(3) *Denials of information requests.* When a data provider denies a request for information pursuant to § 1033.331, the data provider:

(i) Creates a record explaining the basis for the denial; and

(ii) Communicates to the consumer or third party, electronically or in writing, the type(s) of information denied and the reason(s) for the denial, and that the communication occurs as quickly as is practicable.

(c)(1) *Policies and procedures for ensuring accuracy*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface.

(2) *Elements.* In developing its policies and procedures regarding accuracy, a data provider must consider, for example:

(i) Implementing the format requirements of § 1033.311(b); and

(ii) Addressing information provided by a consumer or a third party regarding inaccuracies in the covered data made available through its developer interface.

(3) *Indicia of compliance.* Indicia that a data provider's policies and procedures regarding accuracy are reasonable include whether the policies and procedures conform to a qualified industry standard regarding accuracy.

(d) *Policies and procedures for record retention*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure retention of records that are evidence of compliance with subparts B and C of this part.

(1) *Retention period.* Records related to a data provider's response to a consumer's or third party's request for information or a third party's request to access a developer interface must be retained for at least three years after a data provider has responded to the request. All other records that are evidence of compliance with subparts B and C of this part must be retained for a reasonable period of time.

(2) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under paragraph (a) of this section must include, without limitation:

(i) Records of requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable;

(ii) Records of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable;

(iii) Copies of a third party's authorization to access data on behalf of a consumer; and

(iv) Records of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation mechanism made available by a data provider.

SUBPART D—AUTHORIZED THIRD PARTIES

§ 1033.401 Third party authorization; general.

To become an authorized third party, the third party must seek access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested and:

(a) Provide the consumer with an authorization disclosure as described in § 1033.411;

(b) Provide a statement to the consumer in the authorization disclosure, as provided in § 1033.411(b)(5), certifying that the third party agrees to the obligations described in § 1033.421; and

(c) Obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

§ 1033.411 Authorization disclosure.

(a) *General requirements*. To comply with § 1033.401(a), a third party must provide the consumer with an authorization disclosure electronically or in writing. The authorization disclosure must be clear, conspicuous, and segregated from other material.

(b) *Content.* The authorization disclosure must include:

(1) The name of the third party that will be authorized to access covered data pursuant to the third party authorization procedures in § 1033.401.

(2) The name of the data provider that controls or possesses the covered data that the third party identified in paragraph (b)(1) of this section seeks to access on the consumer's behalf.

(3) A brief description of the product or service that the consumer has requested the third party identified in paragraph (b)(1) of this section provide and a statement that the third party will collect, use, and retain the consumer's data only for the purpose of providing that product or service to the consumer.

(4) The categories of covered data that will be accessed.

(5) The certification statement described in § 1033.401(b).

(6) A description of the revocation mechanism described in § 1033.421(h)(1).

(c) *Language access*—(1) *General language requirements.* The authorization disclosure must be in the same language as the communication in which the third party conveys the authorization disclosure to the consumer. Any translation of the authorization disclosure must be complete and accurate.

(2) *Additional languages.* If the authorization disclosure is in a language other than English, it must include a link to an English-language translation, and it is permitted to include links to translations in other languages. If the authorization disclosure is in English, it is permitted to include links to translations in other languages.

§ 1033.421 Third party obligations.

(a) *General limitation on collection, use, and retention of consumer data*—(1) *In general*. The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service.

(2) *Specific activities.* For purposes of paragraph (a)(1) of this section, the following activities are not part of, or reasonably necessary to provide, any other product or service:

(i) Targeted advertising;

(ii) Cross-selling of other products or services; or

(iii) The sale of covered data.

(b) *Collection of covered data*—(1) *In general*. Collection of covered data for purposes of paragraph (a) of this section includes the scope of covered data collected and the duration and frequency of collection of covered data.

(2) *Maximum duration*. In addition to the limitation described in paragraph (a) of this section, the third party will limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization.

(3) *Reauthorization after maximum duration*. To collect covered data beyond the one-year maximum period described in paragraph (b)(2) of this section, the third party will obtain a new authorization from the consumer pursuant to § 1033.401 no later than the anniversary of the most recent authorization from the consumer. The third party is permitted to ask the consumer for a new authorization pursuant to § 1033.401 in a reasonable manner. Indicia that a new authorization request is reasonable include its conformance to a qualified industry standard.

(4) *Effect of maximum duration*. If a consumer does not provide the third party with a new authorization as described in paragraph (b)(3) of this section, the third party will:

(i) No longer collect covered data pursuant to the most recent authorization; and

(ii) No longer use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service under paragraph (a) of this section.

(c) *Use of covered data.* Use of covered data for purposes of paragraph (a) of this section includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. Examples of uses of covered data that are permitted under paragraph (a) of this section include:

(1) Uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority;

(2) Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and

(3) Servicing or processing the product or service the consumer requested.

(d) *Accuracy.* The third party will establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party, if applicable.

(1) *Flexibility.* A third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities.

(2) *Periodic review.* A third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

(3) *Elements*. In developing its policies and procedures regarding accuracy, a third party must consider, for example:

(i) Accepting covered data in a format required by § 1033.311(b); and

(ii) Addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data.

(4) *Indicia of compliance*. Indicia that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a qualified industry standard regarding accuracy.

(e) *Data security*. (1) A third party will apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801); or

(2) If the third party is not subject to section 501 of the Gramm-Leach-Bliley Act, the third party will apply to its systems for the collection, use, and retention of covered data the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

(f) *Provision of covered data to other third parties*. Before providing covered data to another third party, subject to the limitation described in paragraphs (a) and (c) of this section, the third party will require the other third party by contract to comply with the third party obligations in paragraphs (a) through (g) of this section and the condition in paragraph (h)(3) of this section upon receipt of the notice described in paragraph (h)(2) of this section.

(g) *Ensuring consumers are informed.* (1) The third party will provide the consumer with a copy of the authorization disclosure that is signed or otherwise agreed to by the consumer and reflects the date of the consumer's signature or other written or electronic consent. Upon

obtaining authorization to access covered data on the consumer's behalf, the third party will deliver a copy to the consumer or make it available in a location that is readily accessible to the consumer, such as the third party's interface. If the third party makes the authorization disclosure available in such a location, the third party will ensure it is accessible to the consumer until the third party's access to the consumer's covered data terminates.

(2) The third party will provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. The contact information must be readily identifiable to the consumer.

(3) The third party will establish and maintain reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, the information listed in this paragraph (g)(3) about the third party's access to the consumer's covered data. The third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities, and the third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

(i) Categories of covered data collected;

(ii) Reasons for collecting the covered data;

(iii) Names of parties with which the covered data was shared;

(iv) Reasons for sharing the covered data;

(v) Status of the third party's authorization; and

(vi) How the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation.

(h) *Revocation of third party authorization*—(1) *Provision of revocation mechanism*. The third party will provide the consumer with a mechanism to revoke the third party's authorization

to access the consumer's covered data that is as easy to access and operate as the initial authorization. The third party will also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization.

(2) *Notice of revocation.* The third party will notify the data provider, any data aggregator, and other third parties to whom it has provided the consumer's covered data when the third party receives a revocation request from the consumer.

(3) *Effect of revocation.* Upon receipt of a consumer's revocation request as described in paragraph (h)(1) of this section or notice of a revocation request from a data provider as described in § 1033.331(e), a third party will:

(i) No longer collect covered data pursuant to the most recent authorization; and

(ii) No longer use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service under paragraph (a) of this section.

§ 1033.431 Use of data aggregator.

(a) *Responsibility for authorization procedures when the third party will use a data aggregator.* A data aggregator is permitted to perform the authorization procedures described in § 1033.401 on behalf of the third party seeking authorization under § 1033.401 to access covered data. However, the third party seeking authorization remains responsible for compliance with the authorization procedures described in § 1033.401, and the data aggregator must comply with paragraph (c) of this section.

(b) *Disclosure of the name of the data aggregator.* The authorization disclosure must include the name of any data aggregator that will assist the third party seeking authorization

under § 1033.401 with accessing covered data and a brief description of the services the data aggregator will provide.

(c) *Data aggregator certification.* When the third party seeking authorization under § 1033.401 will use a data aggregator to assist with accessing covered data on behalf of a consumer, the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data in § 1033.421(a) through (f) and the condition in § 1033.421(h)(3) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data. Any data aggregator that is retained by the authorized third party after the consumer has completed the authorization procedures must also satisfy this requirement. For this requirement to be satisfied:

(1) The third party seeking authorization under § 1033.401 must include the data aggregator's certification in the authorization disclosure described in § 1033.411; or

(2) The data aggregator must provide its certification to the consumer in a separate communication.

§ 1033.441 Policies and procedures for third party record retention.

(a) *General requirement.* A third party that is a covered person or service provider, as defined in 12 U.S.C. 5481(6) and (26), must establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the requirements of subpart D.

(b) *Retention period.* Records required under paragraph (a) of this section must be retained for a reasonable period of time, not less than three years after a third party obtains the consumer's most recent authorization under § 1033.401(a).

(c) *Flexibility.* A third party covered under paragraph (a) of this section has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities.

(d) *Periodic review.* A third party covered under paragraph (a) of this section must periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness to evidence compliance with the requirements of subpart D.

(e) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under this section must include, without limitation:

(1) A copy of the authorization disclosure that is signed or otherwise agreed to by the consumer and reflects the date of the consumer's signature or other written or electronic consent and a record of actions taken by the consumer, including actions taken through a data provider, to revoke the third party's authorization; and

(2) With respect to a data aggregator covered under paragraph (a) of this section, a copy of any data aggregator certification statement provided to the consumer separate from the authorization disclosure pursuant to § 1033.431(c)(2).

Consumer Financial Protection Bureau

1700 G Street NW, Washington, D.C. 20552

CFPB Bulletin 2020-01

Date: March 6, 2020

Subject: Responsible Business Conduct: Self-Assessing, Self-Reporting, Remediating, and Cooperating

In executing its statutory responsibilities, the Bureau of Consumer Financial Protection (Bureau) places primary emphasis on preventing harm to consumers. Preventing harm to consumers is among the most effective and efficient ways of ensuring consumer access to a fair, transparent, and competitive financial market. In 2013, the Bureau issued a Bulletin that identified several activities that individuals or businesses, collectively "entities," could engage in that could prevent and minimize harm to consumers, referring to these activities as "responsible conduct." The Bureau is issuing this updated Bulletin to clarify its approach to responsible conduct and to reiterate the importance of such conduct.

In the first instance, the Bureau's focus is on building a culture of compliance among entities, including covered persons and service providers, in order to minimize the likelihood of a violation of Federal consumer financial law, and thereby prevent harm to consumers. When a violation of law does occur, swift and effective actions taken by an entity to address the violation can minimize resulting harm to consumers. Specifically, an entity may self-assess its compliance with Federal consumer financial law, self-report to the Bureau when it identifies likely violations, remediate the harm resulting from these likely violations, and cooperate above and beyond what is required by law with any Bureau review or investigation.

Such activities are in the public interest. Depending on its form and substance, responsible conduct can improve the Bureau's ability to promptly detect violations of Federal consumer financial law, increase the effectiveness and efficiency of its supervisory and enforcement work, enable the Bureau to focus its finite resources on their best use for the mission, and help more consumers in more matters promptly receive financial redress and additional meaningful remedies for any harm they experienced.

Because responsible conduct is in the public interest, the Bureau seeks to encourage it. Accordingly, if an entity meaningfully engages in responsible conduct, the Bureau intends to

favorably consider such conduct, along with other relevant factors, in addressing violations of Federal consumer financial law in supervisory and enforcement matters.[1] Depending on the nature and extent of an entity's actions, the Bureau has a wide range of options available to properly account for responsible conduct. For example, in light of an entity's responsible conduct, the Bureau could exercise its discretion to close an enforcement investigation with no action or decide not to include Matters Requiring Attention in an exam report or supervisory letter. Even if the Bureau does take action, those who engage in responsible conduct may receive other types of credit for engaging in such behavior. For entities within the Bureau's supervisory authority, the Bureau's Division of Supervision, Enforcement, and Fair Lending makes determinations of whether violations should be resolved through non-public supervisory action or a possible public enforcement action through its Action Review Committee (ARC) process. The ARC process includes factors that are closely aligned with the elements of responsible conduct. Thus, for entities under the Bureau's supervisory authority, responsible conduct could result in resolving violations non-publicly through the supervisory process. Responsible conduct also could result in the Bureau's reducing the number of violations pursued or reducing the sanctions or penalties sought by the Bureau in any public enforcement action. The Bureau intends to consider the extent and significance of an entity's responsible conduct, with more extensive and important responsible conduct leading to more substantial consideration.

This guidance, and its description of factors that may warrant favorable consideration, is not adopting any rule or formula to be applied in all matters. The importance of each factor in a given matter, and the way in which the Bureau evaluates each factor, will depend on the circumstances. The Bureau is not in any way limiting its discretion and responsibility to evaluate each matter individually on its own facts and circumstances. In short, the fact that an entity may argue it has satisfied some or even all of the factors set forth in this guidance will not necessarily foreclose the Bureau from bringing any enforcement action or seeking any remedy if it believes such a course is necessary and appropriate.

---

[1] Other factors the Bureau considers in determining how to resolve violations of Federal consumer financial law include, without limitation, (1) the nature, extent, and severity of the violations identified and any associated consumer harm; (2) an entity's demonstrated effectiveness and willingness to address the violations; and (3) the importance of deterrence, considering the significance and pervasiveness of the potential consumer harm.

Factors Used to Evaluate and Acknowledge Responsible Conduct

As noted previously, the Bureau principally considers four categories of conduct when evaluating whether some form of credit is warranted in an enforcement investigation or supervisory matter: self-assessing, self-reporting, remediating, and cooperating. However, if an entity engages in another type of activity particular to its situation that is both substantial and meaningful, the Bureau may take that activity into consideration.

Listed below are some of the factors the Bureau intends to consider in determining whether and how much to take into account responsible conduct. This list is not exhaustive, and some of the factors identified may relate to more than one category of responsible conduct.

Self-assessing:

This factor, which can also be described as self-monitoring or self-auditing, reflects a proactive commitment by an entity to use resources for the prevention and early detection of violations of Federal consumer financial law. The Bureau recognizes that a robust compliance management system appropriate for the size and complexity of an entity's business will not prevent all violations, but it will reduce the risk of violations, and it will often facilitate early detection of likely violations, which can limit the size and scope of consumer harm. Questions the Bureau intends to consider in determining whether to provide favorable consideration for self-assessing activity include:

1. What resources does the entity devote to compliance? How robust and effective is its compliance management system? Is it appropriate for the size and complexity of the entity's business?

2. Has the entity taken steps to improve its compliance management system when deficiencies have been identified either by itself or external regulators? Did the entity ignore obvious deficiencies in compliance procedures? Does the entity have a culture of compliance?

3. Considering the nature of the violation, did the entity identify the issue? What is the nature of the violation or likely violation and how did it arise? Was the conduct pervasive or an isolated act? How long did it last? Did senior personnel participate in, or turn a blind eye toward, obvious indicia of misconduct?

4. How was the violation detected and who uncovered it? If identified by the entity, how did the entity identify the issue (*e.g.*, from customer complaints, audits or monitoring

based on routine risk assessments, or whistleblower activity)? Was the identification the result of a robust and effective compliance management system including adequate internal audit, monitoring, and complaint review processes? Was identification prompted by an impending exam or an investigation by a regulator?

5. What self-assessment mechanisms were in place to effectively prevent, identify, or limit the conduct that occurred, elevate it appropriately, and preserve relevant information? In what ways, if any, were the entity's self-assessing mechanisms particularly noteworthy and effective?

Self-reporting:

This factor substantially advances the Bureau's protection of consumers and enhances its mission by reducing the resources it must expend to identify violations and making those resources available for other significant matters. Prompt self-reporting of likely violations also represents concrete evidence of an entity's commitment to responsibly address the conduct at issue. Conversely, efforts to conceal a likely violation from the Bureau represent concrete evidence of the entity's lack of commitment to responsibly address the conduct at issue. For these reasons, the Bureau considers this factor in its evaluation of an entity's overall conduct. Of note, however, an entity's self-reporting of a potential issue does not require it to concede that it has violated the law. Questions the Bureau intends to examine in determining whether to provide favorable consideration for self-reporting of likely violations of Federal consumer financial law include:

1. Did the entity completely and effectively disclose the existence of the conduct to the Bureau, to other regulators, and, if applicable, to self-regulatory organizations? Did the entity report any additional related misconduct likely to have occurred?

2. Did the entity report the conduct to the Bureau without unreasonable delay? If it delayed, what justification, if any, existed for the delay? How did the delay affect the preservation of relevant information, the ability of the Bureau to conduct its review or investigation, or the interests of affected consumers?

3. Did the entity proactively self-report, or wait until discovery or disclosure was likely to happen anyway, for example due to impending supervisory activity, public company reporting requirements, the emergence of a whistleblower, consumer complaints or actions, or the conduct of a Bureau investigation?

Remediating:

When violations of Federal consumer financial law have occurred, the Bureau's remedial priorities include obtaining full redress for those injured by the violations, ensuring that the entity who violated the law implements measures designed to prevent the violations from recurring, and, when appropriate, effectuating changes in the entity's future conduct for the protection and/or benefit of consumers. Questions the Bureau intends to examine in determining whether to provide favorable consideration for remediation activity regarding likely violations of Federal consumer financial law include:

1. What steps did the entity take upon learning of the violation? Did it immediately stop the violation? How long after the violation was uncovered did it take to implement an effective response?

2. What steps did the entity take to discipline the individuals responsible for the violation and to prevent the individuals from repeating the same or similar conduct?

3. Did the entity conduct an analysis to determine the number of affected consumers and the extent to which they were harmed? Were consumers made whole through compensation and other appropriate relief, as applicable? Did affected consumers receive appropriate information related to the violations within a reasonable period of time?

4. What assurances are there that the violation (or a similar violation) is unlikely to recur? Did the entity take measures, such as a root-cause analysis, to ensure that the issues were addressed and resolved in a manner likely to prevent and minimize future violations? Similarly, have the entity's business practices, policies, and procedures changed to remove harmful incentives and encourage proper compliance?

Cooperating:

Unlike self-assessing and remediating, which may occur with or without Bureau involvement, cooperating relates to the quality of an entity's interactions with the Bureau after the Bureau becomes aware of a likely violation of Federal consumer financial law, either through an entity's self-reporting or the Bureau's own efforts. Credit for cooperating in this context depends on the extent to which an entity takes steps above and beyond what the law requires in its interactions with the Bureau. Simply meeting those legal obligations is not a factor that the Bureau intends to give any special consideration in a supervisory review or enforcement investigation. Of note,

the Bureau does not consider an entity's good faith assertion of privilege in an enforcement investigation to be a lack of cooperation; an entity asserting privileges in good faith remains eligible for potential favorable consideration for cooperating. Questions the Bureau intends to examine in determining whether to provide favorable consideration for cooperating in a Bureau matter include:

1. Did the entity cooperate promptly and completely with the Bureau and other appropriate regulatory and law enforcement bodies? Was that cooperation present throughout the course of the review and/or investigation?

2. Did the entity take proper steps to develop the facts quickly and completely and to fully share its findings with the Bureau? Did it undertake a thorough review of the nature, extent, origins, and consequences of the violation and related behavior? Who conducted the review and did they have a vested interest or bias in the outcome? Were scope limitations placed on the review? If so, why and what were they?

3. Did the entity promptly make available to the Bureau the results of its review and provide sufficient documentation reflecting its response to the situation? Did it provide evidence with sufficient precision and completeness to facilitate, among other things, appropriate actions against others who violated the law? Did the entity produce a complete and thorough written report detailing the findings of its review? Did it voluntarily disclose material information not directly requested by the Bureau or that otherwise might not have been uncovered? Did the entity provide all relevant, non-privileged information and make assertions of privilege in good faith?

4. Did the entity direct its employees to cooperate with the Bureau and make reasonable efforts to secure such cooperation? Did it make the most appropriate person(s) available for interviews, consultation, and/or sworn statements?

The Bureau intends for this guidance to encourage entities subject to the Bureau's supervisory and enforcement authority to engage in more "responsible conduct," as defined herein. Such an outcome, the Bureau believes, would benefit both consumers and providers of consumer financial products and services, is in the public interest, and supports the Bureau's efforts to prevent consumer harm.

Regulatory Requirements

This Bulletin is a non-binding general statement of policy articulating considerations relevant to the Bureau's exercise of its supervisory and enforcement authority. It is therefore exempt from notice and comment rulemaking requirements under the Administrative Procedure Act pursuant to 5 U.S.C. 553(b). Because no notice of proposed rulemaking is required, the Regulatory Flexibility Act does not require an initial or final regulatory flexibility analysis. 5 U.S.C. 603(a), 604(a). The Bureau has determined that this Bulletin does not impose any new or revise any existing recordkeeping, reporting, or disclosure requirements on covered entities or members of the public that would be collections of information requiring OMB approval under the Paperwork Reduction Act, 44 U.S.C. 3501 *et seq*.

Pursuant to the Congressional Review Act, 5 U.S.C. 801 *et seq*., the Bureau will submit a report containing this policy statement and other required information to the United States Senate, the United States House of Representatives, and the Comptroller General of the United States prior to its applicability date. The Office of Information and Regulatory Affairs has designated this policy statement as not a "major rule" as defined by 5 U.S.C. 804(2).