Office of the Comptroller of the Currency

Table of Contents

1. Interagency Statement — Model Risk Management for BSA/AML Compliance
2. Bulletin — Overdraft Protection Programs: Risk Management Practices
3. Bulletin — Legal Lending Limit Guidance
4. Bulletin — Revised Bank Enforcement Manual
5. Bulletin — Cybersecurity Supervision Work Program
6. Announcement — Office of Financial Technology

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
Office of the Comptroller of the Currency

Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance

April 9, 2021

Introduction

The Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies), in consultation with the Financial Crimes Enforcement Network and the National Credit Union Administration, are issuing this statement regarding industry questions on model risk management. This statement addresses how the risk management principles described in the agencies' "Supervisory Guidance on Model Risk Management"[1] (referred to as the "model risk management guidance" or MRMG) relate to systems or models used by banks[2] to assist in complying with the requirements of Bank Secrecy Act laws and regulations.

The MRMG (like all supervisory guidance) does not have the force and effect of law. The agencies support efforts by banks to innovate and update their Bank Secrecy Act/Anti-Money Laundering (BSA/AML) systems and models to quickly adapt to an evolving threat environment. The agencies recognize that not all banks use models such as those described in the MRMG for BSA/AML compliance or have formalized model risk management (MRM) frameworks. This statement is intended to clarify how the MRMG may be a useful resource to guide a bank's MRM framework, whether formal or informal, and assist with BSA/AML compliance. Whether a bank characterizes a BSA/AML system (or portions of that system) as a model, a tool, or an application, risk management of such a system should be consistent with safety and soundness principles[3] and the system should promote compliance with applicable laws and regulations.

This statement does not alter existing BSA/AML legal or regulatory requirements, nor does it establish new supervisory expectations. In addition, this statement does not suggest that a bank change existing risk management practices if the bank uses them to effectively manage its risk.

The MRMG is principles-based and articulates the agencies' general views regarding appropriate practices for MRM. It is intended to assist banks that rely on models to do so in a safe and sound

[1] Refer to the "Supervisory Guidance on Model Risk Management," Federal Reserve SR Letter 11-7; OCC Bulletin 2011-12; and FDIC FIL 22-2017.

[2] The term "bank" is used here as in Bank Secrecy Act regulations at 31 CFR 1010.100(d) other than subsection (d)(6). This interagency statement does not apply to credit unions. The term "bank" as used in this interagency statement does include each agent, agency, branch, or office within the United States of banks, savings associations, and foreign banks.

[3] Refer to the "Interagency Guidelines Establishing Standards for Safety and Soundness," 12 CFR 208, Appendix D-1 (Federal Reserve); 12 CFR 364, Appendix A (FDIC); and 12 CFR 30, Appendix A (OCC).

manner, and in compliance with applicable laws and regulations.[4] The MRMG principles provide flexibility for banks in developing, implementing and updating models, including those used for BSA/AML activities. While the MRMG provides a comprehensive discussion of all aspects of model risk management, the practical application of any principle discussed in the MRMG by a bank depends, in part, on the bank's reliance on, and the nature of, its models. While models used for BSA/AML compliance may be different from other models, appropriate model testing and validation processes typically take these differences into account.

Background

Banks routinely use models for a broad range of activities. Models can help to inform and improve business decisions, save money, and reduce the risks that banks face. The use of models can also impose costs, including the potential for unintended and adverse consequences from decisions based on model output that is either incorrect or misused. As reflected in the MRMG, effective model risk management is important because of the potential for poor business and strategic decisions, financial losses, noncompliance with laws and regulations, or damage to a bank's reputation arising from deficient or misapplied models.

Consistent with a risk-based approach, the rigor and sophistication of sound risk management practices are generally commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations. If the bank's use of models is less prevalent and has less material impact on the bank's financial condition, operations, or compliance, then a less sophisticated approach to MRM may be appropriate. When models and model outputs could have a material impact on business decisions, including decisions related to risk management, and capital and liquidity planning, and when model failure would have a particularly harmful impact on a bank's financial condition, operations, or compliance, a more extensive and robust MRM framework may be appropriate.

BSA/AML Systems and the MRMG

The agencies' BSA program regulations require a bank to have a reasonably designed compliance program[5] that includes, among its components, a system of internal controls to assure ongoing compliance with BSA regulatory requirements. In this context, effective internal controls are typically based on the bank's risk profile.

BSA/AML systems and a bank's policies, procedures, and processes to identify, research, and report unusual activity, commonly known as suspicious activity monitoring and reporting systems, are critical internal controls for ensuring an effective BSA/AML compliance program. BSA/AML systems may include a surveillance monitoring system, sometimes referred to as an automated transaction monitoring system. Some of these automated transaction monitoring systems may involve the use of modeling.

---

[4] Refer to the "Interagency Statement Clarifying the Role of Supervisory Guidance," issued on September 11, 2018, Federal Reserve Supervision and Regulation Letter 18-5, FDIC Financial Institution Letter (FIL)- 49-2018, OCC News Release 2018-97.

[5] 12 CFR 208.63 (Federal Reserve), 12 CFR 326.8(b) and (c) (FDIC), and 12 CFR 21.21 (OCC), require a bank to establish and maintain a BSA/AML compliance program. *See also* 31 CFR 1020.210 (FinCEN).

There is no definition in statute or regulation of what constitutes a model for the purposes of model risk management; however, the MRMG uses the following definition of a model:

> The term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.[6]

The MRMG lists the following three components of a model:

1. An information input component, which delivers assumptions and data to the model.
2. A processing component, which transforms inputs into estimates.
3. A reporting component, which translates the estimates into useful business information.

While some BSA/AML systems may constitute models under this description, others may not. The determination by a bank of whether a BSA/AML system is considered a model is bank-specific, and a conclusion regarding the system's categorization should be based on a consideration of all relevant information. There are no required categorizations of particular BSA/AML systems, including those used to monitor for suspicious activity. Categorizations vary based on the bank's BSA/AML program and the individual features of the bank's BSA/AML systems. The following examples likely would not be considered models, as defined by the MRMG, because they may lack one or more of the three components discussed above:

- Stand-alone, simple tools that flag transactions based on a singular factor, such as reports that identify cash, wire transfer, or other transaction activity over certain value thresholds.
- Systems used to aggregate cash transactions occurring at the bank's branches for the purposes of filing Currency Transaction Reports.

Regardless of whether a bank characterizes a BSA/AML system as a model, a tool, or an application, there is no specific organizational structure required for oversight by the bank. Oversight of BSA/AML systems might be conducted solely by the bank's compliance area, an MRM group, another functional area, or some combination of these functions. Sound risk management and procedures for evaluating the effectiveness of compliance programs are both key components to an effective BSA/AML compliance program.

The MRMG is nonbinding and provides principles that may be helpful in managing the BSA/AML compliance program. There is no requirement or supervisory expectation that banks have duplicative processes for complying with BSA/AML regulatory requirements. For automated transaction monitoring systems, prudent risk management involves periodically[7] reviewing and testing the filtering criteria and thresholds to ensure that they are still effective, as

---

[6] The definition of "model", as described in the MRMG, also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.

[7] Model reviews and validations are generally performed using a risk-based approach, and with a frequency appropriate for (or when there are changes to) a bank's risk profile. BSA/AML risk profile changes may include new or revised bank products, services, customer types, or geographic locations, or if the bank expands through mergers and acquisitions. Material changes to models likely warrant validation.

well as independently validating the monitoring system's methodology and effectiveness to ensure that the monitoring system is detecting potentially suspicious activity.

Further, there is no requirement that a bank perform duplicative independent testing activities, including model validation, to ensure compliance with BSA/AML regulations. In certain cases, validation conducted on models may help a bank in its independent testing for BSA/AML purposes; similarly, some aspects of independent testing for BSA/AML purposes may assist a bank in its model validation activities. Generally, the principles for risk management set forth in the MRMG provide a framework that can be used to help support an effective BSA compliance program.

Model risk management includes disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy.[8] In the context of BSA/AML systems that are considered by a bank to be models, sound model development and validation activities typically align with the purpose of each model and incorporate model objectives, structure, data, methodologies, complexity, and extent of use. The extent and nature of model risk varies across models and banks, and a bank's risk management framework is most appropriately tailored when it is commensurate with the nature and materiality of the risk. For example, a bank's MRM framework may support the implementation of less material changes to models without revalidation, or with the revalidation of certain model components without revalidating the entire model, in appropriate circumstances. Overall, the statements contained within the MRMG are meant to provide useful information for the bank's consideration and are not to be regarded as "templates" or requirements.

The MRMG describes how banks may objectively assess model risk using a sound model validation process, including evaluation of conceptual soundness, ongoing monitoring, and outcomes analysis. A central principle for managing model risk is "effective challenge" of models, which refers to critical analysis by objective, informed parties. For banks that use models to comply with the BSA/AML requirements, it is important that validation be performed by individuals with sufficient expertise and an appropriate level of independence from the model's development and implementation. An appropriate level of independence for individuals performing model validation is also important when banks outsource multiple functions to the same third party.

The agencies recognize that the objectives and structure of BSA/AML models (BSA/AML systems determined by a bank to be models) may differ from those in other business units because the objectives of most BSA/AML models place greater emphasis on coverage over efficiency. BSA/AML models may require quick adjustments to reflect the changing nature of criminal behavior or the bank's risk profile. Similarly, testing and performance monitoring for some BSA/AML models may not include the same techniques as other models because of various factors, such as the lack of information about realized outcomes (e.g., Suspicious Activity Reports). The MRMG notes that the nature of testing and model assessment can vary across models and recognizes that for some models complete information may not be available. A bank's validation methodology may take such differences into account. For example, a bank

[8] The systems, processes, models, or tools used by a bank for BSA/AML purposes must be consistent with relevant laws and regulations.

may choose to accept a reduction in efficiency (such as by producing more alerts) in exchange for greater coverage in its automated transaction monitoring system. Banks typically make these decisions based on risk and change or update controls, as appropriate, to ensure that effective controls are in place.

Third-Party Models

Third-party models can assist banks in improving the efficacy of their BSA/AML programs, and reasonable due diligence prior to entering into a contractual relationship with a third party is important to a successful relationship. In addition, ongoing monitoring of the third party and the model is important when a bank depends on a third-party model for compliance-related activities, such as currency transaction reporting, monitoring transactions, detection of suspicious activity, or suspicious activity reporting.

Banks are ultimately responsible for complying with BSA/AML requirements, even if they choose to use third-party models to assist with their BSA/AML compliance programs. In doing so, banks may consider the principles discussed in the agencies' third-party risk management issuances and the aspects of the MRMG that address third-party models.[9] Although the proprietary nature of third-party models is a consideration, sound risk management practices include obtaining sufficient information from the third party to understand how the model operates and performs, ensuring that it is working as expected, and tailoring its use to the unique risk profile of the bank. These practices assist in meeting BSA/AML regulatory compliance requirements.[10]

An understanding of how the third-party model operates is important to the bank's ability to effectively negotiate contracts that will protect the bank's needs and rights, including needs and rights concerning privacy and information security. In addition, it is important that banks using third-party models have contingency plans if the third-party model is no longer available or serviced or may no longer be reliable.

Conclusion

In summary, the extent and nature of model risk varies across models and banks, and effective risk management is commensurate with the nature and materiality of the risk. The agencies are clarifying, in this statement, the following points:

- The MRMG, like all supervisory guidance, does not have the force and effect of law. Banks may use some or all of the principles in the MRMG in their risk management processes to support meeting the regulatory requirements of an effective BSA/AML compliance program. Banks with limited model use may not have formal MRM frameworks.

---

[9] Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance" (OCC), OCC Bulletin 2020-10, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29" (OCC); SR 13-19 (Federal Reserve); and FDIC FIL-44-2008, "Guidance for Managing Third-Party Risk" for more information regarding third-party risk management.

[10] Refer to the agencies' third-party risk management issuances noted in footnote 8 and the discussion of third-party models in the MRMG for more information.

- The MRMG is not meant to serve as a set of testing procedures, including with regard to BSA/AML systems.

- The MRMG does not establish any requirements or supervisory expectations that banks have duplicative processes for complying with BSA/AML regulatory requirements.

- Certain processes and systems used in BSA/AML compliance may not be models. The determination by a bank of whether a system used for BSA/AML compliance is considered a model is bank-specific. When making this determination, a bank may consider the MRMG model definition and the three components that characterize models.

- Banks assess different models in different ways. The nature of testing and analysis of models depends on the type of model and the context in which the models are used.

- The MRMG principles provide flexibility for banks in developing, implementing, and updating models. Banks may benefit from employing this flexibility, including for validation activities, to update BSA/AML models quickly in response to the evolving threat environment and to implement innovative approaches. Banks may establish policies that govern when the bank may implement less material changes to models without revalidation, or may choose to revalidate certain model components without revalidating the entire model.

- Banks may choose to use a third-party model. When doing so, banks may consider the principles discussed in the agencies' third-party risk management issuances and the aspects of the MRMG that address third-party models.

- Regardless of how a BSA/AML system is characterized, sound risk management is important, and banks may use the principles discussed in the MRMG to establish, implement, and maintain their risk management framework.

OCC Bulletin 2023-12 | April 26, 2023

Overdraft Protection Programs: Risk Management Practices

To

Chief Executive Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

The Office of the Comptroller of the Currency (OCC) is issuing this bulletin to banks[1] to address the risks associated with overdraft protection programs.[2] Overdraft protection programs can present a variety of risks, including compliance, operational, reputation, and credit risks.[3] Specifically, this bulletin discusses certain practices that may present heightened risk of violating prohibitions against unfair or deceptive acts or practices.

The bulletin also describes practices that may assist banks with managing overdraft protection program risks. When supported by appropriate risk management practices, overdraft protection programs may assist some consumers in meeting short-term liquidity and cash-flow needs. The OCC recognizes that some banks have announced changes to their overdraft protection programs that may be consistent with appropriate risk management practices.

This bulletin's focus is consistent with the OCC's mission to ensure that banks operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations. This bulletin also furthers the OCC's support for innovation by banks to meet the evolving needs of consumers, businesses, and communities.

Note for Community Banks

This bulletin applies to community banks that offer overdraft protection programs.

Highlights

This bulletin

- provides background information on overdraft protection programs.
- addresses certain practices that may result in heightened risk exposure, including the risk of violating section 5 of the Federal Trade Commission (FTC) Act (Section 5), which prohibits unfair or deceptive acts or practices,[4] and Section 1036 of the Consumer Financial Protection Act of 2010, which prohibits unfair, deceptive, or abusive acts or practices.[5] These practices include
  - assessing overdraft fees on debit card transactions that are authorized when a consumer's available account balance is positive but later post to the account when the available balance is negative, also referred to as "authorize positive, settle negative" (APSN).
  - assessing an additional fee each time a third party resubmits the same transaction for payment after a bank returns the transaction for non-sufficient funds (NSF) (referred to as "representment fees").
- describes certain practices that may help to manage risks associated with overdraft protection programs, including
  - assisting consumers in avoiding unduly high costs in relation to the face value of the item being presented, the amount of their regular deposits, and their average account balances.
  - implementing fees and practices that bear a reasonable relationship to the risks and costs of providing overdraft protection program services.

Background

The OCC and other agencies set out safety and soundness considerations, legal risks, and best practices for overdraft protection programs in the "Joint Guidance on Overdraft Protection Programs" (2005 Guidance) conveyed by OCC Bulletin 2005-9, "Overdraft Protection Programs: Interagency Guidance." The agencies issued the 2005 Guidance to address concerns raised by institutions, financial supervisors, and the public about the marketing, disclosure, and implementation of overdraft protection programs. Since 2005, the OCC has observed significant developments in the consumer banking landscape, such as

- changes in overdraft protection program-related legal requirements[6] and consumer behavior, including the increased and more frequent use of overdrafts as, in effect, a form of short-term credit.
- overdraft protection programs resulting in consumers paying high costs relative to the face value of items being presented and to deposit amounts and average account balances.

The OCC continues to observe evolution in the consumer banking landscape, such as

- banks offering deposit accounts that do not allow overdrafts.
- banks offering deposit accounts with no fees for overdrafts.
- banks reducing the amount of overdraft fees in existing overdraft protection programs.
- ongoing efforts by banks and other stakeholders to identify opportunities for modifying existing overdraft protection programs in ways to manage the risks of such programs.

The OCC encourages banks to explore offering low-cost accounts, as well as other lower-cost alternatives for covering overdrafts, such as overdraft lines of credit and linked accounts. The OCC recognizes, however, that some consumers with short-term liquidity needs may benefit from the availability of funds from overdraft protection programs via deposit accounts.

Based on examinations of overdraft protection programs at a number of banks in recent years, the OCC has observed that certain overdraft protection program practices may present a heightened risk of violations of Section 5.[7] These include practices known as APSN and representment fees.[8]

Authorize Positive, Settle Negative Fee Practices

Banks generally maintain a "ledger balance" and an "available balance" on customer deposit accounts for numerous purposes, including assessing overdraft fees. The ledger balance refers to the actual amount of funds in a customer's deposit account after accounting for all items that have settled and posted. The available balance generally reflects the ledger balance minus "holds" for recently deposited funds that have not yet cleared and for authorized but pending debit card transactions. Some banks assess overdraft fees on debit card transactions that authorize when a customer's available balance is positive but that later post to the account when the available balance is negative.

In this scenario, a customer's account has a sufficient available balance to cover a debit card transaction when the transaction is authorized but, due to one or more intervening transactions, has an insufficient available balance to cover the transaction at the time it settles.[9] This is commonly referred to as an APSN transaction. In addition to assessing an overdraft fee on the APSN transaction, some banks also assess an overdraft fee on intervening transactions that exceed the customer's available balance. In this scenario, for example, the bank reduces a customer's available balance by an amount that is more than, equal to, or less than the initial authorized debit card transaction, and subsequently, an intervening transaction further reduces the customer's available balance so that the account no longer has a sufficient available balance. The bank charges an overdraft fee on both the intervening transaction and the initial APSN transaction when posted to the customer's account.[10]

The OCC has reviewed a number of overdraft protection programs that assess overdraft fees on APSN transactions. In some instances, the OCC has found account materials to be deceptive, for purposes of Section 5, with respect to the banks' overdraft fee practices.[11] In these instances, misleading disclosures contributed to findings that the APSN practice was also unfair for purposes of Section 5. In addition, and

based on subsequent analysis, even when disclosures described the circumstances under which consumers may incur overdraft fees, the OCC has found that overdraft fees charged for APSN transactions are unfair for purposes of Section 5 because consumers were still unlikely to be able to reasonably avoid injury and the facts met the other factors for establishing unfairness.[12]

The OCC recognizes that compliance risk may exist when banks assess overdraft fees based on either a negative ledger balance or negative available balance for APSN transactions.[13]

Representment Fee Practices

When a bank receives a check or automated clearing house (ACH) transaction that is presented for payment from a customer's deposit account, and the account has insufficient funds to pay the check or ACH transaction, the bank may decline to pay the transaction and charge the customer an NSF fee. If the same check or ACH transaction is presented to the bank again and the customer's account still has insufficient funds, some banks will either again return the transaction unpaid and assess an additional NSF fee or pay the transaction and assess an overdraft fee. This practice of charging an additional fee each time a single transaction (e.g., ACH transaction or check) is presented for payment by a third party without further action by the customer contributes to customer costs in circumstances in which those customers cannot reasonably avoid the additional charges.[14] Through ongoing supervision, the OCC has identified concerns with a bank's assessment of an additional fee on a representment transaction, resulting in findings in some instances that the practice was unfair and deceptive. Disclosures may be deceptive, for purposes of Section 5, if they do not clearly explain that multiple or additional fees (NSF or overdraft) may result from multiple presentments of the same transaction. Even when customer disclosures explain that a single check or ACH transaction may result in more than one fee, a bank's practice of assessing fees on each representment may also be unfair, for purposes of Section 5, if consumers cannot reasonably avoid the harm and the other factors for establishing unfairness under Section 5 are met. Consumers typically have no control over when a returned ACH transaction or check will be presented again and lack knowledge of whether an intervening deposit will be sufficient to cover the transaction and related fees.

Additional Practices That May Present Heightened Risk

- **High limits or lack of daily limits on the number of fees assessed:** In the OCC's supervisory experience, charging overdraft or NSF fees with a high limit (or without limit) for multiple transactions in a single day has contributed to determinations that banks' overdraft protection programs as a whole were unfair for purposes of Section 5 because the lack of limits results in high costs for consumers and difficulty in bringing accounts positive.
- **Sustained overdraft fees:** In the OCC's supervisory experience, charging a fixed, periodic fee for failure to cure a previous overdrawn balance has contributed to findings of unfairness and deception, for purposes of Section 5, especially when the bank does not accurately disclose the

circumstances under which the customer could incur these fees. These practices make it more difficult for customers facing liquidity challenges to reasonably avoid these fees by bringing their account balances positive.

Risk Management Practices

A bank's risk management systems should be commensurate with the bank's size, complexity, and risk profile. Therefore, as part of sound risk management of overdraft protection programs, the OCC encourages a bank to assess and analyze the risks posed by the bank's overdraft protection program activities; adjust the bank's risk management practices; and incorporate oversight of overdraft protection programs into the bank's compliance management system. An effective compliance management system typically should include processes and practices designed to manage compliance risk, ensure compliance with applicable laws and regulations, and prevent consumer harm.[15]

Board and Management Oversight

A bank's board of directors has ultimate responsibility for overseeing management's implementation of a bank's overdraft protection program. Effective board and management oversight generally includes

- setting and confirming the bank's strategic approach and risk appetite for offering overdraft protection programs.
- providing guidance to senior management.
- ensuring that the bank has an effective change management process.
- performing ongoing monitoring to self-identify and self-correct weaknesses.
- monitoring the program's performance and measures relative to the bank's objectives and risk appetite.
- periodically reviewing information on a bank's overdraft protection program, including an assessment of customer impacts and overdraft product analyses to confirm that these services are fair and transparent.
- ensuring proper and accurate customer disclosures.

Bank management is responsible for developing, implementing, and effectively managing overdraft protection programs in line with the board's direction, the bank's objectives, and the bank's risk appetite, and in compliance with all applicable laws and regulations. Sound risk management generally should include appropriate policies, processes, personnel, and control systems that focus on consumer protection requirements and consider customer outcomes.[16]

New Activities Processes and Third-Party Risk Management

Banks should have processes in place to manage the risks associated with offering new, modified, or expanded products or services (collectively, new activities), including new overdraft protection programs or changes to existing overdraft protection programs. Effective new activity development processes typically consider the financial attributes of consumers using the products, consumer disclosures, use of new technologies, use of alternative underwriting information, and use of third-party relationships. An effective risk management program should be in place if banks use third-party relationships as part of their overdraft protection programs.[17] Third-party relationships include a bank's arrangement with its service providers that often play a significant role in processing and reprocessing transactions, processing of payments, and providing systems that determine when overdraft or NSF fees are assessed.[18]

Policies, Processes, and Control Systems

A bank's processes and control systems should align with established policies and incorporate appropriate procedures and practices for managing risks associated with overdraft protection programs. The following non-exhaustive list outlines examples of potentially appropriate risk management practices that banks may consider adopting:

- **Eligibility:** Overdraft limits and account agreement terms that are aligned with eligibility and underwriting criteria that promote fair treatment and fair access. Product structures, including short-term single payment structures, support consumer affordability and successful repayment of negative account balances in a reasonable time frame rather than reliance on regular or repeated reborrowing.
- **Opt-in status:** Policies and procedures that fully comply with the requirements of 12 CFR 1005.17 for one-time debit card and automated teller machine transactions. Policies and procedures should address compliance with these requirements. For other types of transactions (e.g., paper checks and recurring ACH or debit card transactions), consumers are provided the opportunity to affirmatively opt in to and opt out of overdraft protection at any time.[19]
- **Consumer disclosures:** Disclosures that effectively convey policies and practices related to accounts and products offered to consumers via transparent, understandable, and timely communication of account features. These disclosures support informed decision making with regard to overdraft protection programs and their related costs. Banks periodically test operating system settings and parameters to determine whether transaction postings are aligned to disclosures.
- **Overdraft protection product analysis:** A process for reviewing data and analyzing whether overall overdraft protection program revenues are reasonably related to the product risks and costs, as appropriate, at the portfolio, account, and transaction levels. Such analyses can also inform (1) modifications to overdraft protection programs intended to support a bank's longer-term competitive position, consumer satisfaction levels, and customer retention activities; and (2) a

bank's evaluation of the effect of any implemented modifications.

- **Periodic account analysis:** Processes to periodically review accounts of customers who use overdraft protection programs on a regular basis. The objectives of this review are primarily to confirm that customers
  - are provided with readily accessible and understandable tools and information to assist in managing their finances.
  - are not routinely relying on overdraft protection programs.
  - receive fair treatment.
  - are not incurring disproportionate costs relative to the face value of the item being presented, the amount of their regular deposits, and their average account balances.
- **Account monitoring:** Periodic account analyses that result in appropriate changes to overdraft limits, eligibility for continued use, or recommendations to consumers for other appropriate deposit account services when overreliance, excessive costs, or options for more cost-effective credit usage are detected. Overdraft limits and any changes to overdraft limits are clearly and timely communicated to consumers.
- **Grace amounts:** Grace amounts, or de minimis exclusions from fees that are based on transaction size or the magnitude of the overdrawn balance, are meaningful and periodically reviewed.
- **Grace periods:** Grace periods that provide additional time before the assessment of fees sufficient for customers to address a potential or actual negative account balance through an additional deposit or transfer of funds.
- **Online access and timely automated alerts:** Processes to send consumers accurate information in real or near real time through online account access or electronic alerts, such as text messages, online or web-based applications, or emails. In certain circumstances, these technologies may provide opportunities for customers to react to and address negative balances or items being presented for settlement to avoid fees.
- **Single daily fee:** Single daily fee assessments that are reasonably related to the costs of providing either overdraft protection or returned item for NSF services, offer effective transparency to customers, and eliminate confusion caused by item-posting order protocols or the use of available account balances.
- **Timing of fee collection:** A practice of collecting fees related to overdraft protection or NSF services from the next deposit only after all other appropriately presented items have posted or cleared to ensure that a greater amount of the consumers' deposited funds is available for consumer use.
- **Complaints management:** Incorporating overdraft protection-related complaints into a bank's complaint management and resolution processes,[20] which should be commensurate with the bank's size, complexity, and risk profile. Processes should include steps to analyze complaint data and to detect and remediate concerns or problem areas, including potential unfair or deceptive

acts or practices or unfair, deceptive, or abusive acts or practices.[21]

Corrective Action

The OCC encourages banks to have processes in place to identify and correct risk management weaknesses and violations of laws and regulations. OCC violation findings at specific banks related to overdraft protection programs have typically led to corrective action, including remediation to harmed consumers. The OCC encourages banks to review their overdraft protection programs and related practices to ensure that banks comply with Section 5 and other applicable laws and regulations and take corrective action as appropriate.

Further Information

Please contact Candace B. Matzenauer, Director for Consumer Compliance Policy, at (202) 649-5470, or Terence W. Culler, Director for Retail Credit Risk Policy, at (202) 649-6670.

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

---

[1] "Banks" refers collectively to national banks, federal savings associations, covered savings associations, and federal branches and agencies of foreign banking organizations.

[2] This bulletin focuses on automated, discretionary overdraft services for which banks charge fees, rather than the types of products or services described in 12 CFR 1005.17(a)(1)–(4).

[3] Refer to the "Deposit-Related Credit" booklet of the *Comptroller's Handbook* for an overview of the primary risks associated with deposit-related credit generally.

[4] Refer to 15 USC 45(a)(1).

[5] Refer to 12 USC 5536.

[6] For more information, refer to OCC Bulletin 2010-15, "Overdraft Protection: Opt-In Requirements and Related Marketing Issues."

[7] Refer to OCC Advisory Letter 2002-3, "Guidance on Unfair or Deceptive Acts or Practices," for applicable legal standards the OCC uses to evaluate whether an act or practice violates the prohibition on unfair or deceptive acts or practices in Section 5 of the FTC Act.

[8] For information on how the APSN practice relates to the Consumer Financial Protection Act's prohibition on unfair acts or practices (12 USC 5536), refer to the Consumer Financial Protection Bureau's Consumer Financial Protection Circular 2022-06, "Unanticipated Overdraft Fee Assessment Practices" (October 26, 2022).

[9] As used here, the term "intervening transaction" means a transaction that a bank authorizes for payment or that settles against a customer's account after the debit card transaction is authorized but before it posts to the customer's account. For an example, refer to table 1 in CFPB Circular 2022-06.

[10] Refer to table 2 in CFPB Circular 2022-06.

[11] OCC Advisory Letter 2002-3 states that a practice may be found to be deceptive and thereby unlawful under Section 5 if the following

three factors are present (1) there is a representation, omission, act, or practice that is likely to mislead; (2) the act or practice would be deceptive from the perspective of a reasonable consumer; and (3) the representation, omission, act, or practice is material.

[12] OCC Advisory Letter 2002-3 states that a practice may be found to be unfair and thereby unlawful under Section 5 if (1) the practice causes substantial consumer injury; (2) the injury is not outweighed by benefits to the consumer or to competition; and (3) the injury caused by the practice is one that consumers could not reasonably have avoided.

[13] Refer to, for example, *CFPB Supervisory Highlights*, "Junk Fees Special Edition," Issue 29, at 4 (Winter 2023).

[14] For information on unfairness factors, refer to OCC Advisory Letter 2002-3.

[15] For more information, refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook*.

[16] For more information, refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* and the *Director's Book: Role of Directors for National Banks and Federal Savings Associations*.

[17] For more information, refer to OCC Bulletin 2020-10, "Frequently Asked Questions to Supplement OCC Bulletin 2013-29," and OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance."

[18] For more information, refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles," and OCC Bulletin 2019-62, "Consumer Compliance: Interagency Statement on the Use of Alternative Data in Credit Underwriting."

[19] For more information, refer to OCC Bulletin 2010-15.

[20] For more information, refer to the "Compliance Management Systems" booklet of the *Comptroller's Handbook*.

[21] For more information, refer to the "Unfair or Deceptive Acts or Practices and Unfair, Deceptive, or Abusive Acts or Practices" booklet of the *Comptroller's Handbook*.

OCC Bulletin 2023-27 | August 8, 2023

Loan Purchase Activities: Legal Lending Limit Guidance

To

Chief Executive Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

The Office of the Comptroller of the Currency (OCC) is issuing this bulletin to provide banks[1] with guidance regarding the applicability of the legal lending limit (LLL) to purchased loans.

Note for Community Banks

This bulletin applies to community banks' purchases of loans.

Highlights

This bulletin

- provides background information on loan purchase activities and the LLL.
- provides guidance on the applicability of the LLL to purchased loans and types of recourse arrangements.

Background

Loan purchase activities are long-standing banking practices that serve the legitimate business needs of the buying and selling institutions and the public interest. The extensive network of loan-broker channels and increased involvement of nonbank lenders have resulted in growth in the availability of

loans for purchase.[2]

Unless an exception applies, all loans and extensions of credit made by banks are subject to the LLL, which provides limitations on the total amount of loans and extensions of credit to any one borrower.[3] Whether a loan that a bank purchases is attributable to the seller under the LLL regulation depends on specific facts and circumstances. Consequently, bank management would typically consider more information than it would for in-house originations when determining compliance with the LLL regulation for purchased loans.

Guidance

Aggregate exposures attributable to a single seller must be within the bank's LLL. Loans are attributable to a seller under 12 CFR 32.2(q)(1)(iii) if the bank has direct or indirect recourse to the seller. Direct or indirect recourse can be explicit or implied. Explicit recourse is generally provided under contractual arrangement or other written agreement between the bank and the seller. Implied recourse is established through the bank's course of dealing[4] or conduct with a seller even if the contract or written agreement with the provider does not contain explicit recourse. The following are examples of explicit and implied recourse scenarios:

- **Explicit recourse:** Examples include a requirement or contractual obligation to substitute or repurchase defaulted loans or refill a reserve account, even if no substitutions, repurchases, or replenishments of the reserve account have occurred to date.
- **Implied recourse:** Examples include when the seller has routinely substituted or repurchased loans or refilled or replenished a reserve account even when the contract does not require those actions.

If the bank does not have explicit or implied recourse to the seller, the loans are generally not attributable to the seller under 12 CFR 32.2(q)(1)(iii). In such cases, the purchased loans would generally be attributable under the LLL regulation to only the named borrowers on the loans, unless the direct benefit or common enterprise tests under 12 CFR 32.5 are met or other provisions under the LLL regulation warrant attribution to another party.[5]

Further Information

Please contact your OCC supervisory office.

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

[1] "Banks" refers collectively to national banks, federal savings associations, and federal branches and agencies of foreign banking organizations.

[2] For additional information on loan purchase activities, refer to OCC Bulletin 2020-81, "Credit Risk: Risk Management of Loan Purchase Activities."

[3] The LLL statute is 12 USC 84, "Lending Limits," for national banks and 12 USC 1464(u), "Limits on Loans to One Borrower," for federal savings associations. 12 USC 84 applies to federal savings associations pursuant to 12 USC 1464(u). The regulation for national banks and federal savings associations is 12 CFR 32, "Lending Limits." "Loans and extensions of credit" are defined in 12 CFR 32.2(q). 12 CFR 32.3(a) provides the combined general limit; 12 CFR 32.3(b) provides loans and extensions of credit that are subject to special lending limits; and 12 CFR 32.3(c) provides loans and extensions of credit that are not subject to the LLL.

[4] Section 1-303 of the Uniform Commercial Code and section 223 of the Restatement (Second) of Contracts (1981) generally describe a course of dealing as a sequence of previous conduct between the parties to an agreement or a particular transaction that is fairly regarded as establishing a common basis of understanding for interpreting their expressions and other conduct. A course of dealing may give meaning to certain terms or supplement or qualify the terms of an agreement.

[5] The direct benefit and common enterprise tests under the combination rules are separate and distinct from 12 CFR 32.2(q)(1)(iii). A loan is subject to the direct benefit and common enterprise tests under the 12 CFR 32.5 combination rules independent of its attribution to a seller under 12 CFR 32.2(q)(1)(iii).

Topic(s): LEGAL LENDING LIMITS ▪ PARTICIPATIONS SYNDICATIONS

OCC Bulletin 2023-16 | May 25, 2023

OCC Enforcement Actions: Revised Policies and Procedures Manual for Bank Enforcement Actions and Related Matters

To

Chief Executive Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

The Office of the Comptroller of the Currency (OCC) today released a revised *Policies and Procedures Manual* (PPM) for bank enforcement actions and related matters. This revised version of PPM 5310-3 replaces the version issued on November 13, 2018.

Rescission

This bulletin rescinds OCC Bulletin 2018-41, "OCC Enforcement Actions: OCC Enforcement Action Policies and Procedures Manuals," issued on November 13, 2018.

Note for Community Banks

These policies and procedures apply to all OCC-supervised banks.[1]

Highlights

PPM 5310-3, "Bank Enforcement Actions and Related Matters," now includes a new appendix, "Appendix C: Actions Against Banks With Persistent Weaknesses." The new appendix discusses

- persistent weaknesses a bank may exhibit warranting further action(s) by the OCC against the bank.
- the types of actions, requirements, and restrictions that may be appropriate to address a bank's persistent weaknesses.

Background

In November 2018, the OCC updated its policies and procedures regarding bank enforcement actions and related matters with the issuance of a revised PPM 5310-3. The 2023 revision of the PPM includes a new appendix C, which generally applies to banks subject to Heightened Standards under 12 CFR 30, appendix D. The new appendix includes information about the OCC's consideration of supervisory and enforcement actions against banks that exhibit persistent weaknesses, including banks with highly complex operations that have failed to correct persistent weaknesses. Appendix C describes enforcement actions the OCC will consider, which could include additional requirements and restrictions, such as requirements that a bank acquire or hold additional capital or liquidity or restrictions on the bank's growth, business activities, or payment of dividends. If a bank has failed to correct its persistent weaknesses in response to prior enforcement actions or other measures, then the OCC will consider further action. Such action could require the bank to simplify or reduce its operations including that the bank reduce its asset size, divest subsidiaries or business lines, or exit from one or more markets of operation.

The revised PPM also incorporates additional clarifications, including updated legal and regulatory citations.

The OCC's enforcement policies reflect the principles important in implementing the OCC's mission to ensure that national banks and federal savings associations operate in a safe and sound manner, provide fair access to financial services, treat customers fairly, and comply with applicable laws and regulations.

Further Information

Please contact the OCC's Enforcement group at (202) 649-6200 or Specialty Supervision Division at (202) 649-6450.

Beverly Cole
Senior Deputy Comptroller for Midsize and Community Bank Supervision

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

Greg J. Coleman
Senior Deputy Comptroller for Large Bank Supervision

Benjamin W. McDonough
Senior Deputy Comptroller and Chief Counsel

Related Link

- PPM 5310-3, "Bank Enforcement Actions and Related Matters" (PDF)

---

[1] "Banks" refers collectively to national banks, federal savings associations, covered savings associations, and federal branches and agencies of foreign banking organizations.

Topic(s): ENFORCEMENT ACTIONS EXAMINATIONS

OCC Bulletin 2023-22 | June 26, 2023

Cybersecurity: Cybersecurity Supervision Work Program

To

Chief Executive Officers of All National Banks, Federal Savings Associations, and Federal Branches and Agencies; Department and Division Heads; All Examining Personnel; and Other Interested Parties

Summary

The Office of the Comptroller of the Currency (OCC) recently developed and distributed the Cybersecurity Supervision Work Program for use by examiners. As cyberattacks evolve and as banks[1] adopt various standardized tools and frameworks to assess cybersecurity preparedness, the OCC recognized the need to update its approach to cybersecurity assessment as part of the agency's bank supervision. The Cybersecurity Supervision Work Program (CSW) provides high-level examination objectives and procedures that are aligned with existing supervisory guidance and the National Institute of Standards and Technology Cybersecurity Framework. The CSW Overview page on www.occ.gov links to the CSW References page, which provides cross-references that map the CSW procedures to existing supervisory guidance and industry cybersecurity frameworks. For example, cross-references include the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, the Center for Internet Security's Critical Security Controls, and the Cyber Risk Institute's Profile.

The CSW does not establish new regulatory expectations, and banks are not required to use this work program to assess cybersecurity preparedness. The OCC continues to encourage but does not require use of standardized approaches to assess and improve cybersecurity preparedness, and banks may choose from a variety of tools and frameworks available.[2] The CSW does not change the availability of banks' optional use of the FFIEC Cybersecurity Assessment Tool or other cybersecurity frameworks.

Note for Community Banks

Examiners may use the CSW's examination procedures during examinations of a community bank's cybersecurity preparedness.

Highlights

The CSW

- is designed to more effectively address evolving risks and support risk-based bank information technology examinations.
- is aligned with the National Institute of Standards and Technology Cybersecurity Framework.
- is informed by the *FFIEC Information Technology Examination Handbook* and common cybersecurity frameworks.
- is designed to focus on cybersecurity preparedness and supplements the OCC's bank information technology examination procedures contained in the "Community Bank Supervision," "Large Bank Supervision," and "Federal Branches and Agencies Supervision" booklets of the *Comptroller's Handbook*.

Further Information

Please contact Norine Richards, Director of Bank Information Technology Policy at (202) 649-6550.

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

Related Links

- "Cybersecurity Supervision Work Program" (PDF)
- Cybersecurity Supervision Work Program Overview
- Cybersecurity Supervision Work Program References

---

[1] "Banks" refers collectively to national banks, federal savings associations, covered savings associations, and federal branches and agencies of foreign banking organizations.

[2] Refer to Federal Financial Institution Examination Council press release titled "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," August 28, 2019.

Topic(s): BANK INFORMATION TECHNOLOGY (BIT) BANK OPERATIONS INFORMATION & CYBER SECURITY - BIT

News Release 2023-31 | March 30, 2023

OCC Establishes Office of Financial Technology

WASHINGTON—The Office of the Comptroller of the Currency (OCC) today announced the establishment of its Office of Financial Technology and the selection of Prashant Bhardwaj to lead the office as Deputy Comptroller and Chief Financial Technology Officer, effective April 10, 2023.

In October 2022, the OCC announced that it would expand upon its Office of Innovation and establish an Office of Financial Technology in early 2023 to bolster the agency's expertise and ability to adapt to the rapid pace of technological changes in the banking industry. The Office of Financial Technology broadens the OCC's focus in this area and ensures the agency's leadership and agility in providing high-quality supervision of bank-fintech partnerships. It further enhances

the agency's knowledge and expertise of financial technology platforms and applications in support of the OCC's mission.

In his role as Deputy Comptroller and Chief Financial Technology Officer, Mr. Bhardwaj will lead the team responsible for analysis, evaluation, and discussion of relevant trends in financial technology, emerging and potential risks, and the potential implications for OCC supervision. The Office will enhance the OCC's expertise on matters regarding digital assets, fintech partnerships, and other changing technologies and business models within and that affect OCC-supervised banks.

Mr. Bhardwaj joins the agency after nearly 30 years of experience serving in a variety of roles across the financial sector.

He holds a master's degree in accounting from University of Cincinnati and a master's degree in business administration from the International Management Institute Universiade de Brussels.

Media Contact

Stephanie Collins
(202) 649-6870

Topic(s):
- OFFICE OF FINANCIAL TECHNOLOGY