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

July 25, 2024

Joint Statement on Banks' Arrangements with Third Parties to Deliver Bank Deposit Products and Services

The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the agencies) are issuing this statement to note potential risks related to arrangements between banks and third parties[1] to deliver bank deposit products and services to end users.[2] This statement highlights examples of risk management practices by banks to manage such risks. This statement reemphasizes existing guidance; it does not alter existing legal or regulatory requirements or establish new supervisory expectations.

The agencies support responsible innovation and support banks in pursuing third-party arrangements in a manner consistent with safe and sound practices and in compliance with applicable laws and regulations, including, but not limited to, those designed to protect consumers (such as fair lending laws and prohibitions against unfair, deceptive, or abusive acts or practices) and those addressing financial crimes (such as fraud and money laundering). Banks are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation.

Some banks have entered into arrangements with third parties to deliver deposit products and services (such as checking and savings accounts) to end users. Banks may do this in order to increase revenue, raise deposits, expand geographic reach, or to achieve other strategic objectives, including by leveraging new technology or offering innovative products and services. In these arrangements, a third party, rather than the bank, typically markets, distributes or otherwise provides access to or facilitates the provision of the deposit product or service directly to the end user.[3] In some arrangements, banks rely on one or multiple third parties to maintain the deposit and transaction system of record; process payments (sometimes with the ability to directly submit payment instructions to payment networks); perform regulatory compliance functions; provide end-user facing technology applications; service accounts; perform customer service; and perform complaint and dispute resolution functions. These third parties are sometimes referred to as intermediate platform providers, processors, middleware providers, aggregation layers, and/or program managers. A bank's use of third parties to perform certain activities does not diminish its responsibility to comply with all applicable laws and regulations.

[1] These sometimes include non-bank companies, such as, but not limited to, certain financial technology (or fintech) companies.

[2] For purposes of this statement, an "end user" includes consumers and businesses accessing deposit products and services through the arrangements described in this statement.

[3] These arrangements are sometimes referred to as "banking-as-a-service" or "embedded finance" depending on the structure and parties involved in the arrangement.

Similar structures have been utilized for certain activities in the banking industry for many years, such as activities related to prepaid card programs. However, the agencies have observed an evolution and expansion of these arrangements to include more complex arrangements that involve the reliance on third parties to deliver deposit products and services.

POTENTIAL RISKS

Depending on the structure, third-party arrangements for the delivery of deposit products and services can involve elevated risks. The agencies have observed that risks may be elevated in certain circumstances, such as the examples below.

Operational and Compliance

- *Significant operations performed by a third party:* Substantially relying on third parties to manage a bank's deposit operations can eliminate or reduce a bank's crucial existing controls over and management of the deposit function. Without adequate initial due diligence and ongoing monitoring, risks to the integrity of a bank's deposit function are heightened.[4]
- *Fragmented operations:* Fragmented operational functions for deposit products and services among multiple third parties may make it more difficult for the bank to effectively assess risks and assess whether all third parties can and do perform assigned functions as intended.
- *Lack of access to records:* A potential lack of sufficient access by a bank to the deposit and transaction system of record and other crucial information and data maintained by the third party can impair the bank's ability to determine its deposit obligations. In some circumstances, such uncertainty can lead to delays in end-users' access to their deposits, which in turn can expose the bank to additional legal and compliance risks.
- *Third parties performing compliance functions:* Reliance on third parties to perform regulatory compliance functions may increase the risk of the bank not meeting its regulatory requirements. Specifically, the third party may perform certain regulatory compliance functions such as monitoring and reporting suspicious activity, customer identification programs, customer due diligence, and sanctions compliance on behalf of the bank. Regardless of whether the functions are shared between the bank and the third party, the bank remains responsible for failure to comply with applicable requirements.
- *Insufficient risk management to meet consumer protection obligations:* Insufficient oversight of these arrangements may impact a bank's compliance with consumer protection laws and regulations, such as requirements under Regulation E (implementing the Electronic Fund Transfer Act) to investigate and resolve certain payment disputes within required

[4] Depending on the structure, such arrangements may also introduce security vulnerabilities, including by providing another access point into the bank's systems. Integration may amplify operational risks, such as fraud, cybersecurity, and data privacy incidents occurring at the third party that then affect the bank.

timeframes, and under Regulation DD (implementing the Truth in Savings Act) to provide certain disclosures regarding consumer deposit accounts. Presenting insufficient or misleading information to end users also may result in violations of laws and regulations, including consumer protection requirements.[5] In addition, inadequate complaint administration and error resolution processes may limit a bank's ability to effectively identify and address issues impacting end users of the deposit accounts and result in potential consumer harm.

- *Lack of contracts:* Multiple levels of third-party and subcontractor relationships, where the bank does not have direct contracts with entities that perform crucial functions may pose challenges to the bank's ability to identify, assess, monitor, and control various risks.
- *Lack of experience with new methods:* Arrangements leveraging new technologies or new methods of facilitating deposit products and services with which bank management and staff do not have prior experience may result in inadequate risk and compliance management practices to manage or oversee these arrangements and associated risks.
- *Weak audit coverage:* Lack of sufficient audit scope and coverage, follow-up processes, and remediation may result in inadequate oversight of these arrangements and reduce the effectiveness of the audit function.

Growth

- *Misaligned incentives:* A third party's incentives may not be aligned with those of the bank, such as when a third party may be incentivized to promote growth in a manner that is not aligned with the bank's regulatory obligations, resulting in insufficient attention to risk management and compliance obligations.
- *Operational capabilities lag growth:* Rapid growth as a result of these arrangements (either in the overall number of arrangements or in the size of specific arrangements) may result in risk management and operational processes struggling to keep pace.
- *Financial risks from funding concentrations:* Arrangements may result in significant and rapidly increasing funding concentrations, which may make it more challenging for the bank to manage and mitigate liquidity and funding risks, particularly when funding is deployed in illiquid or long-term assets.
- *Inability to manage emerging liquidity risks:* Arrangements where a significant proportion of a bank's deposits or revenue are associated with a third party may pose liquidity risks, such that the bank may be reluctant to make decisions necessary to manage those risks, including, if necessary, to terminate the arrangement.

[5] Such laws and regulations include (among others) the prohibition against unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act, and the prohibition against unfair, deceptive, or abusive acts or practices under Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).

- *Pressure on capital levels:* Arrangements may result in material and rapid balance sheet growth (including significant intraday balance sheet levels) without commensurate capital formation.

End User Confusion and Misrepresentation of Deposit Insurance Coverage

- *Potentially misleading statements and marketing:* Third-party arrangements for the delivery of deposit products and services can pose risks of end user confusion related to deposit insurance, which may be exacerbated by marketing materials or other statements by nonbank third parties. Some nonbank third parties could be reasonably mistaken for an insured depository institution (IDI) by end users, particularly when they refer to FDIC deposit insurance in marketing and other public-facing materials. End users may not be aware that access to their funds may depend on the third party and that deposit insurance does not protect against losses resulting from the failure of the third party.
- *Regulatory violations:* Inaccurate or misleading information regarding the extent or manner under which deposit insurance coverage is available could constitute a violation under Part 328, Subpart B.[6]
    - Omissions of material information also may constitute misrepresentations under the FDIC's rule. Such deposit insurance misrepresentations may occur, for example, when nonbank third parties have communicated to end users that their funds are FDIC insured, without disclosing that FDIC insurance protects only against the failure of an IDI, and not against the failure of the nonbank entity.
    - Deposit insurance misrepresentations under Part 328 may also occur when parties to these arrangements communicate to end users that their funds are insured by the FDIC on a pass-through basis without disclosing that certain regulatory requirements[7] must be satisfied for pass-through deposit insurance coverage to apply.[8]

RISK MANAGEMENT AND GOVERNANCE CONSIDERATIONS

Banks are expected to operate in a safe and sound manner and in compliance with applicable laws and regulations, including those related to safety and soundness, consumer protection, and anti-money laundering/countering the financing of terrorism (AML/CFT). Effective board and

[6] See 12 CFR 328, Subpart B.

[7] See 12 CFR 330.5, 330.7. For pass-through deposit insurance to apply, a consumer's funds must first be on deposit at an IDI. In addition: (1) the deposit account records of the IDI must disclose a basis for pass-through coverage, such as a custodial or agency relationship; (2) the identities and interests of the actual owners of the funds must be ascertainable either from the records of the IDI or records maintained in good faith and in the regular course of business by another party; and (3) the relationship that provides the basis for pass-through deposit insurance coverage must be genuine, with the deposited funds actually owned by the named owners. Additional requirements apply to arrangements involving multiple levels of relationships.

[8] See 12 CFR 328.102(b)(5).

senior management oversight is crucial to ensure a bank's risk management practices are commensurate with the complexity, risk, size, and nature of the activity and relationship, both when the relationship commences and as it evolves over time. In this regard, banks should ensure practices are consistent with the Interagency Guidelines Establishing Standards for Safety and Soundness,[9] and banks also are encouraged to review and consider the risk management principles for third-party relationships set forth in the Interagency Guidance on Third-Party Relationships: Risk Management.[10] The list at the end of this document provides various existing resources, including guidance, that may be helpful for banks managing such arrangements.

The agencies have observed examples of effective risk management practices that a bank may consider when managing third-party arrangements for the delivery of deposit products and services, including the examples below.[11]

Governance and Third-Party Risk Management[12]

- Developing and maintaining appropriate policies and procedures that detail organizational structures, lines of reporting and authorities, expertise and staffing, internal controls, and audit functions to ensure that risks are understood and mitigated.
- Developing appropriate risk assessments that identify and analyze risks specific to features of each arrangement. This practice is important to allow the bank to assess whether proposed controls can appropriately mitigate risks in keeping with the bank's risk appetite. Effective risk assessments typically involve expertise across relevant functional areas of the bank including risk management and compliance, and also consider the activities and features specific to an arrangement to assist in implementing effective controls.

---

[9] See Interagency Guidelines Establishing Standards for Safety and Soundness 12 CFR part 30, Appendix A (OCC); 12 CFR part 208, Appendix D-1 (Board); and 12 CFR part 364, Appendix A (FDIC) (issued pursuant to section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1) (hereinafter "Safety and Soundness Standards").

[10] Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37,920 (June 9, 2023) (hereinafter "TPRM").

[11] These examples are not a complete list of practices that could be considered in managing the risks of such arrangements.

[12] These risk management practices are drawn from applicable statutes, rules, and enforceable guidelines including the Safety and Soundness Standards, *supra* n. 9, and Interagency Guidelines Establishing Information Security Standards, 12 CFR part 30, Appendix B (OCC); 12 CFR part 208, Appendix D-2 (Board); and 12 CFR part 364, Appendix B (FDIC) (issued pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 and 6805, and section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1) (hereinafter "Information Security Standards"), as well as existing guidance and resources, including TPRM, *supra* n. 10; Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks (August 27, 2021) (hereinafter "Community Bank Guide"); and FFIEC Information Technology Examination Handbook (hereinafter "FFIEC IT Examination Handbook").

- Conducting and documenting due diligence that is of sufficient scope and depth to determine whether the bank can rely on third parties to perform the various necessary roles to deliver deposit products and services on the bank's behalf.
- Entering into contracts and agreements that clearly define roles and responsibilities of banks and third parties and enable banks to manage the risks of the arrangements effectively.
- Assessing potential risks when the bank does not have a direct contractual relationship with all parties with significant roles to determine whether and how such risks can be sufficiently mitigated and remain consistent with the bank's risk appetite.
- Establishing effective ongoing monitoring processes, commensurate with the risk of each activity and relationship, and sufficient to detect any issues so they can be addressed in a timely manner.

Managing Operational and Compliance Implications[13]

- Maintaining a clear understanding of any management information system (MIS)[14] that will be used to support the activity, including any obligations and contractual reporting requirements when the deposit and transaction system of record is managed through the third party or through a subcontractor to another party.
- Developing and maintaining risk-based contingency plans, which address potential operational disruption or business failure at the third party that may disrupt end users' access to funds, including contractual provisions that facilitate the bank's contingency plans. The contract might, for example, address the transfer of the relevant accounts, data, or activities to another entity in the event of the third party's bankruptcy, business failure, business interruption, or failure to perform as expected.
- Implementing internal controls to mitigate risks inherent in deposit functions. These could include, but are not limited to, dual control and separation of duties, payment data verification, and clear error processing and problem resolution procedures. When deposit-related functions are performed by a third party, due diligence, contracts, and ongoing monitoring can allow the bank to assess accuracy, reliability, and timeliness of controls and records.
- Establishing adequate policies, procedures, oversight, and controls to help ensure the bank complies with applicable laws and regulations, including consumer protection requirements.

---

[13] These risk management practices are drawn from applicable statutes, rules, and enforceable guidelines including the Safety and Soundness Standards, *supra* n. 9, and Information Security Standards, *supra* n. 12, as well as existing guidance and resources, including TPRM, *supra* n. 10; Community Bank Guide, *supra* n. 12; FFIEC IT Examination Handbook, *supra* n. 12; and Interagency Guidance on Deposit Reconciliation Practices (May 18, 2016).

[14] In arrangements where the third party manages the MIS, a bank may consider potential risks to the bank (such as consumer harm, business disruptions due to partner default, and access to/receipt of MIS), any potential implications to compliance with applicable laws and regulations, and appropriate mitigation measures. A bank may typically consider factors such as the third party's ability to maintain the confidentiality, availability, and integrity of the bank's systems, information, and data, as well as customer data, where applicable.

Effective compliance management includes conducting active oversight of third-party relationships; ensuring effective complaint management, error investigation and resolution; maintaining written policies and procedures; ensuring appropriate consumer protection-related disclosures; and managing a potential disruption of service.[15]

Anti-Money Laundering (AML) / Countering the Financing of Terrorism (CFT) / Sanctions Compliance[16]

- Having adequate policies, procedures, oversight, and controls to help ensure the bank complies with applicable AML/CFT requirements (e.g., monitoring for and reporting suspicious activity, customer identification programs, and customer due diligence) and sanctions compliance.

Managing Growth, Liquidity, and Capital Implications[17]

- Establishing appropriate concentration limits, diversification strategies, liquidity risk management strategies, and exit strategies, as well as maintaining capital adequacy. This may include contingency funding plans that describe how the bank will respond to customers' unexpected deposit withdrawals and reasonable assumptions, such as non-maturity deposit customer behavior.
- Performing appropriate analysis to determine whether parties involved in the placement of deposits meet the definition of a deposit broker under 12 U.S.C. 1831f and implementing regulations, 12 CFR 337.6, and appropriately reporting any such deposits as brokered deposits in the Call Report.[18]

[15] For example, banks are generally required to make funds available according to specific time schedules and to disclose their funds availability policies to their customers.

[16] These risk management practices are drawn from applicable law and regulations, including 31 CFR 1010.230, 1020.220; 12 CFR 21.11, 208.62, 353; and the Office of Foreign Assets Control sanctions established under the Trading with the Enemy Act, 50 U.S.C. App. 1-44, and other relevant authorities.

[17] These risk management practices are drawn from applicable statute, rules, and enforceable guidelines including 12 U.S.C. 1831f; 12 CFR 337.6; Safety and Soundness Standards, *supra* n. 9; as well as existing guidance and resources, including Interagency Policy Statement on Funding and Liquidity Risk Management, 75 Fed. Reg. 13,656 (March 22, 2010) and Joint Agency Policy Statement: Interest Rate Risk, 61 Fed. Reg. 33,166 (June 26, 1996).

[18] Less than well capitalized institutions under the respective Prompt Corrective Action provisions have restrictions on their ability to accept, renew, or roll over brokered deposits. 12 CFR 337.6(a)(3), (b).

Addressing Misrepresentations of Deposit Insurance Coverage[19]

- Establishing policies and procedures and developing prudent risk management practices for certain deposit-related arrangements to ensure compliance with 12 CFR 328, Subpart B, which prohibits misrepresentation of deposit insurance.[20]
- Ensuring such policies and procedures include, as appropriate, provisions related to monitoring and evaluating activities of persons that facilitate access to the bank's deposit-related services or products to other parties, as required under Part 328.

[19] See 12 CFR part 328, which applies to IDIs (provisions effective on April 1, 2024, with an extended compliance date of January 1, 2025).

[20] See 12 CFR 328.8.

RESOURCES

- Interagency Guidelines Establishing Standards for Safety and Soundness, 12 CFR part 30, Appendix A (OCC); 12 CFR part 208, Appendix D-1 (Board); and 12 CFR part 364, Appendix A (FDIC).
- Interagency Guidelines Establishing Information Security Standards, 12 CFR part 30, Appendix B (OCC); 12 CFR part 208, Appendix D-2 (Board); and 12 CFR part 364, Appendix B (FDIC).
- Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37,920 (June 9, 2023), https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf, FDIC FIL-29-2023, https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html; Board SR 23-4, https://www.federalreserve.gov/supervisionreg/srletters/SR2304.htm, CA 24-2, https://www.federalreserve.gov/supervisionreg/caletters/caltr2402.htm; OCC Bulletin 2023-17, https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html.
- Third-Party Risk Management: A Guide for Community Banks (May 2024), FDIC FIL-19-2024, https://www.fdic.gov/news/financial-institution-letters/third-party-risk-management-guide-community-banks; Board SR 24-2 / CA 24-1, https://www.federalreserve.gov/supervisionreg/srletters/SR2402.htm; OCC Bulletin 2024-11, https://www.occ.gov/news-issuances/bulletins/2024/bulletin-2024-11.html.
- Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks (August 27, 2021), FDIC FIL-59-2021, https://www.fdic.gov/news/financial-institution-letters/2021/fil21059.html; Board SR 21-15 / CA 21-11, https://www.federalreserve.gov/supervisionreg/srletters/sr2115.htm; OCC Bulletin 2021-40, https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-40.html.
- Interagency Guidance on Deposit Reconciliation Practices (May 18, 2016), FDIC FIL-35-2016, https://www.fdic.gov/news/financial-institution-letters/2016/fil16035.html; Board CA 16-2, https://www.federalreserve.gov/supervisionreg/caletters/caltr1602.htm; OCC Bulletin 2016-16, https://www.occ.gov/news-issuances/bulletins/2016/bulletin-2016-16.html.
- Interagency Policy Statement on Funding and Liquidity Risk Management, 75 Fed. Reg. 13,656 (March 22, 2010), https://www.govinfo.gov/content/pkg/FR-2010-03-22/pdf/2010-6137.pdf, FDIC FIL-13-2010, https://www.fdic.gov/news/financial-institution-letters/2010/fil10013.html; Board SR 10-6, https://www.federalreserve.gov/boarddocs/srletters/2010/sr1006.htm; OCC Bulletin 2010-13, https://www.occ.gov/news-issuances/bulletins/2010/bulletin-2010-13.html.
- Advisory on Interest Rate Risk Management (January 6, 2010), https://www.ffiec.gov/pdf/pr010710.pdf, FDIC FIL-2-2010, https://www.fdic.gov/news/financial-institution-letters/2010/fil10002.html; Board SR 10-1, https://www.federalreserve.gov/boarddocs/srletters/2010/sr1001.htm; OCC Bulletin 2010-1, https://www.occ.gov/news-issuances/bulletins/2010/bulletin-2010-1.html; see also Frequently Asked Questions (January 12, 2012), https://www.ffiec.gov/PDF/01-12RR_FAQs.pdf.
- Joint Agency Policy Statement: Interest Rate Risk, 61 Fed. Reg. 33,166 (June 26, 1996), https://www.govinfo.gov/content/pkg/FR-1996-06-26/pdf/96-16300.pdf, FDIC FIL-52-96,

https://www.fdic.gov/news/financial-institution-letters/1996/fil9652.html; Board SR 96-13, https://www.federalreserve.gov/boarddocs/srletters/1996/sr9613.htm.

- Sound Practices to Strengthen Operational Resilience (November 2, 2020), FDIC FIL-103-2020, https://www.fdic.gov/news/financial-institution-letters/2020/fil20103.html; Board SR 20-24, https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm; OCC Bulletin 2020-94, https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-94.html.
- Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (December 3, 2018), FDIC FIL-79-2018, https://www.fdic.gov/news/financial-institution-letters/2018/fil18079.html; Board SR 18-10, https://www.federalreserve.gov/supervisionreg/srletters/sr1810.htm; OCC Bulletin 2018-44, https://www.occ.gov/news-issuances/bulletins/2018/bulletin-2018-44.html.
- Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence (July 6, 2022), FDIC FIL-28-2022 https://www.fdic.gov/news/financial-institution-letters/2022/fil22028.html; Board SR 22-05, https://www.federalreserve.gov/supervisionreg/srletters/SR2205.htm; OCC Bulletin 2022-18, https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-18a.pdf.
- Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards (March 21, 2016), FDIC FIL-21-2016, https://www.fdic.gov/news/financial-institution-letters/2016/fil16021.html; Board SR 16-7, https://www.federalreserve.gov/supervisionreg/srletters/sr1607.htm; OCC Bulletin 2016-10, https://www.occ.treas.gov/news-issuances/bulletins/2016/bulletin-2016-10.html.
- Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (April 26, 2005), FDIC FIL-32-2005, https://www.fdic.gov/news/financial-institution-letters/2005/fil3205.html; Board SR 05-8, https://www.federalreserve.gov/boarddocs/srletters/2005/sr0508.htm; OCC Bulletin 2005-19, https://www.occ.gov/news-issuances/bulletins/2005/bulletin-2005-19.html.
- FDIC FIL-15-2024: Collecting Identifying Information Required Under the Customer Identification Program (CIP) Rule (March 28, 2024), https://www.fdic.gov/news/financial-institution-letters/2024/fil24015.html.
- Unfair or Deceptive Acts or Practices by State-Chartered Banks (March 11, 2004), FDIC FIL-26-2004: https://www.fdic.gov/news/financial-institution-letters/2004/fil2604.html; Board CA 04-2, https://www.federalreserve.gov/boarddocs/press/bcreg/2004/20040311/attachment.pdf.
- OCC Advisory Letter 2002-3: Guidance on Unfair or Deceptive Acts or Practices, https://www.occ.treas.gov/news-issuances/advisory-letters/2002/advisory-letter-2002-3.pdf.
- FDIC FIL-35-2022: Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies (July 29, 2022), https://www.fdic.gov/news/financial-institution-letters/2022/fil22035.html.
- FDIC Banker Resource Center – Third-Party Relationships, https://www.fdic.gov/resources/bankers/third-party-relationships/.
- Deposit Broker's Processing Guide (updated April 15, 2024), https://www.fdic.gov/deposit/deposits/brokers/index.html.

- Board, Community Bank Access to Innovation through Partnerships, SR 21-16 / CA 21-13 (September 9, 2021), https://www.federalreserve.gov/supervisionreg/srletters/SR2116.htm.
- Board, Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion, SR Letter 16-11 (revised February 17, 2021), https://www.federalreserve.gov/supervisionreg/srletters/SR1611a1.pdf.
- OCC Bulletin 2017-43: New, Modified, or Expanded Bank Products and Services: Risk Management Principles (October 20, 2017), https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-43.html.
- Board, Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing, SR 13-1 / CA 13-1 (January 23, 2013), https://www.federalreserve.gov/supervisionreg/srletters/sr1301.htm.
- Examination Resources:
    - FFIEC Information Technology Examination Handbook, https://ithandbook.ffiec.gov.
    - FFIEC BSA/AML Examination Manual, https://bsaaml.ffiec.gov/manual.
    - Electronic Funds Transfer Act Examination Procedures (Interagency), FDIC FIL 09-2019, https://www.fdic.gov/sites/default/files/2024-03/fil19009b.pdf; Board CA 19-6, https://www.federalreserve.gov/supervisionreg/caletters/caltr1906.htm; OCC Bulletin 2021-33, https://www.occ.gov/publications-and-resources/publications/comptrollers-handbook/files/electronic-fund-transfer-act/pub-ch-efta.pdf.