Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

March 2026

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation

Office of Inspector General

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this OIG Top Management and Performance Challenges Report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

Date: March 26, 2026

Memorandum To: Board of Directors

/S/
From: Jennifer L. Fain
Inspector General

Subject Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

During the past year, the Federal Government, including the Federal Deposit Insurance Corporation (FDIC), has undergone significant restructuring and reform that continues to unfold. Our annual reporting of the Top Management and Performance Challenges facing the FDIC highlights areas that we believe warrant the FDIC's continued attention as it carries out its critical mission and briefly assesses the Agency's progress in addressing those challenges. By statute, the FDIC Office of Inspector General (OIG) is required to conduct this assessment for inclusion in the FDIC's Annual Performance and Accountability Report.

The Top Challenges that we identify below are based on the status, makeup, and processes in place at the FDIC as of mid-February 2026. They are based on our independent oversight through audits, evaluations, investigations, and reviews; discussions with FDIC management at all levels; inquiries and trends from our OIG Hotline; and other credible external sources. We acknowledge that the FDIC is likely to undergo significant changes going forward that may impact these currently identified Top Challenges.

We identified eight Top Management and Performance Challenges facing the FDIC:

1. Optimizing the FDIC Workforce
2. Maintaining a Safe and Accountable Workplace Culture
3. Strengthening Organizational Governance
4. Sustaining Readiness to Execute Resolution and Receivership Responsibilities
5. Ensuring Effective Supervision
6. Improving Contract Management
7. Enhancing Cyber and Data Security
8. Identifying and Combating External Fraud and Misrepresentation

The FDIC OIG will continue to provide independent oversight and serve the American people by preventing, deterring, and detecting waste, fraud, abuse, and misconduct in FDIC programs and operations; and will promote economy, efficiency and effectiveness at the FDIC.

We are unwavering in our commitment to deliver credible results that drive meaningful change, enhance integrity and accountability, and foster public trust in the FDIC.

Top Management and Performance Challenges
2025

The Federal Government continues to undergo significant restructuring and reform. As such, the Federal Deposit Insurance Corporation (FDIC) has experienced substantial change over the past year, including the departure of several senior executives. Since the last Top Management and Performance Challenges (TMPC) report,[1] the President has nominated and the Senate has confirmed the Acting Chairman, Travis J. Hill, to be the 23rd Chairman of the FDIC after serving in an acting capacity for nearly a year. Two new Board Members representing the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB) are also currently in place.[2] Throughout these leadership changes, the FDIC's mission remains essential to the stability of the banking sector and public trust and confidence in the U.S. financial system.

The long-term success of the FDIC depends on a sufficient cadre of skilled personnel, a safe and accountable workplace, effective governance and interdivisional coordination, resolution and receivership readiness, effective supervision, adherence to established internal controls, strong information security, and identification of fraud risks within the banking industry. Maintaining public confidence and the FDIC's role in ensuring financial and banking system stability remain essential priorities. This TMPC report highlights areas requiring close attention as the FDIC navigates recent changes and the eight challenges that we list below:

1. Optimizing the FDIC Workforce
2. Maintaining a Safe and Accountable Workplace Culture
3. Strengthening Organizational Governance
4. Sustaining Readiness to Execute Resolution and Receivership Responsibilities
5. Ensuring Effective Supervision
6. Improving Contract Management
7. Enhancing Cyber and Data Security
8. Identifying and Combating External Fraud and Misrepresentation

These eight areas were informed by our audits, evaluations, reviews, hotline complaints, investigations, as well as other relevant reports. The FDIC OIG will continue to provide independent oversight and serve the American people by preventing and detecting waste,

[1] FDIC OIG, *Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (TMPC-03-2025) (March 2025).

[2] The FDIC is managed by a five-member Board of Directors that includes a Chairman, a Vice Chairman, the Comptroller of the Currency, the Director of the CFPB, and an appointive Director. No more than three members of the Board can belong to the same political party.

fraud, and abuse relating to the FDIC's programs and operations, and promoting economy, efficiency, and effectiveness in the FDIC's operations and programs.

We are unwavering in our commitment to deliver credible results that drive meaningful change, enhance integrity and accountability, and maintain public trust in the FDIC.

Optimizing the FDIC Workforce

Effective human capital is the foundation of any strong government agency. Without effective human capital, agencies risk achieving their mission goals. At the time of our last TPMC report issued in March 2025, the Federal Government was undergoing significant restructuring and reform. Federal employees, including those at the FDIC, were offered the Deferred Resignation Program (DRP). New presidential directives required agencies to freeze hiring, align functions with statutory mandates, prepare for large-scale reductions in force, and limit future hiring to one new employee for every four departures. These measures marked a shift from growing the FDIC workforce after large bank failures in 2023 to active downsizing.

For the FDIC, these changes interact with previously identified human capital risks, particularly in succession management and filling mission-critical positions. Our audits previously concluded that ongoing staff attrition raised concerns about the FDIC's capacity to maintain sufficient skilled personnel for statutorily required examinations and to execute the resolution and receivership activities for failed financial institutions effectively. The full effect of the FDIC's workforce restructuring remains unknown, as these activities are ongoing and therefore present a continued challenge. The OIG plans to revisit and report on the FDIC's efforts in this area as progress continues.

Human Capital Risks and Workforce Challenges

According to the FDIC, the Agency experienced a 20 percent reduction in staff in 2025, transitioning from over 6,300 employees to just over 5,000 as of January 1, 2026.[3] This reduction included 593 FDIC employees who accepted the Deferred Resignation Program, 289 employees who took an offer under the Voluntary Early Retirement Authority or Voluntary Separation Incentive Payment option, and 481 other separations that resulted in large part from natural attrition, including retirements. Throughout 2025, 1,424 FDIC employees were eligible to retire – representing almost a quarter of the FDIC's workforce. As of February 15, an additional 17 percent (or 797) of the remaining FDIC staff were eligible for retirement in 2026. These figures highlight the scale of organizational transformation at the FDIC and the continued need for succession planning.

While organizational transformation can provide opportunities for the FDIC to reshape its business processes, realize efficiencies, and promote employee growth, management should continue to monitor the impact of staffing changes. Relative to the examiner workforce, the FDIC should continue to assess examination processes and maintain a cadre of skilled examiners. According to the FDIC, the proposed number of examiners will enable the FDIC to continue to fully meet its statutory requirements to conduct full scope examinations in 2025

[3] FDIC, *2026 Operating Budget* (December 2025).

and beyond. The reduction in risk examiners includes positions that were eliminated in 2025 due to the government-wide DRP and certain vacancies and reflects the continuing decline in the number of supervised institutions. The FDIC has further proposed reductions for 2026 due to changes the FDIC made to its Continuous Examination Program, which will involve fewer targeted reviews and fewer dedicated examiners at institutions with between $10 billion and $30 billion in assets. With respect to consumer compliance supervision, as part of its workforce optimization, the FDIC reduced examination frequency for most institutions with assets between $350 million and $3 billion, with a concomitant reduction in compliance examiner staffing requirements.

Safety and soundness examinations are essential tools for identifying and mitigating unforeseen risks in the banking sector and helping to protect the Deposit Insurance Fund (DIF). Although the FDIC's *Quarterly Banking Profile for the 3rd quarter of 2025* reflected a generally healthy sector, with strong earnings, widening margins, solid capital, and a declining number of problem banks, vulnerabilities in certain portfolios persist, such as commercial real estate, auto loans, and credit cards, where past due and nonaccrual levels remain elevated. Unknown risks could emerge rapidly, requiring enhanced supervision and more frequent, rigorous examinations. Sustaining this vigilance depends on maintaining a workforce with the requisite expertise and skills.

The impact of staff attrition extends beyond numbers; it can affect institutional knowledge, readiness for resolution and receivership activity, and the ability to respond to crises. In 2025, the Division of Resolutions and Receiverships (DRR) and the Division of Complex Institution Supervision and Resolution (CISR) also experienced organizational transformation. DRR experienced 22-percent staff attrition, and 28 percent of its remaining staff are retirement eligible in 2026. CISR also lost over 20 percent of its staff in 2025, with significant losses in its Resolution Readiness Branch. FDIC support Divisions for information technology (IT), contracting, administrative, financial, and legal services that play an important role during bank failures also faced reductions. As recommended in our resolution and readiness report, establishing and implementing an agency-wide resource committee to monitor and report on corporate resource needs, including existing recruiting strategies, staffing levels, and information technology resources would help strengthen resource planning and response capabilities.

Looking ahead, it is imperative for the FDIC to continue to engage in long-term workforce planning. The current 3-year training period for new examiners underscores the importance of forward-looking workforce strategies. In our memorandum, *FDIC Succession Management and Employee Retention Efforts* (June 2025), we highlighted several governance challenges related to workforce planning. The absence of executive sponsorship, clear governance structures, and defined roles has hindered the development of a centrally managed program. Data governance,

coordinated contracting, and IT infrastructure require immediate attention to support organization-wide succession and retention initiatives. As federal directives continue to reshape the workforce landscape, the FDIC must maintain a sustained focus on strategic workforce planning to ensure its continued effectiveness and mission fulfillment.

Maintaining a Safe and Accountable Workplace Culture

Concerns about a toxic workplace culture at the FDIC emerged in November 2023 and continued into 2025, drawing increased attention from both internal and external stakeholders. The primary issues identified were persistent harassment and inappropriate behavior over several years, ineffective reporting mechanisms and widespread fear of retaliation, and lack of meaningful disciplinary action for misconduct.

In response, we initiated two projects in December 2023 to address these allegations and concerns regarding the FDIC's culture, sexual harassment, and other forms of misconduct. The first project focused on evaluating the effectiveness of the FDIC's sexual harassment prevention program. The second project examined broader cultural and systemic failures (Part 1) and specifically investigated the conduct of certain members of senior leadership (Part 2).

- In our report, *FDIC's Sexual Harassment Prevention Program* (July 2024), we found that the FDIC had not established an effective program to encourage reporting or to consistently investigate and address allegations of sexual harassment. This environment of distrust was exacerbated by the FDIC's inability to sustain many improvements recommended in our earlier report, *Preventing and Addressing Sexual Harassment* (July 2020).

- In our report, *Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct—Part 1* (December 2024), we found a majority of the 2,300 employee survey respondents reported feeling safe, valued, and respected, with generally positive views of co-workers and immediate managers. However, more than one-third said they had experienced or witnessed harassment. FDIC management could not always provide complete information about disciplinary actions, and there was no agency-wide policy on penalties or recommended ranges to ensure fair and consistent discipline. Additionally, policies did not require reporting of allegations of harassment involving employees to the Chairman or Board of Directors, leaving senior executives without sufficient information to address the problems effectively.

- In our report, *Special Inquiry of the FDIC's Workplace Culture with Respect to Harassment and Related Misconduct—Part 2* (July 2025), preliminary evidence led to investigations of harassment and misconduct allegations against five senior officials. While the severity of misconduct varied, evidence showed that each official engaged in some degree of inappropriate workplace behavior. Certain actions failed to protect victims and did not consistently align with the FDIC's policies and core values, such as accountability, fairness, and integrity. The investigations also validated FDIC employee perceptions described in Part 1. Many employees believed the Agency would not

effectively implement its action plan because some executives leading the efforts had allegations against them. Evidence showed that three senior officials assisted each other in discreetly and quickly resolving complaints when misconduct allegations arose.

During fiscal year (FY) 2025, the FDIC made considerable progress in addressing the findings in these reports, taking corrective actions to close several recommendations to improve its anti-harassment program and workplace culture. In November 2025, the FDIC reported making a number of noteworthy changes in its *Report on Culture Transformation*.

Importantly, the FDIC created two independent offices, each reporting to the FDIC Board of Directors: the Office of Professional Conduct (OPC) and Office of Equal Employment Opportunity (OEEO). OPC intakes, investigates, oversees (and in some cases decides) discipline, and defends disciplinary appeals for complaints of harassment, interpersonal misconduct, and retaliation for reporting such misconduct. OEEO investigates and reports on complaints of discrimination under the laws enforced by the Equal Employment Opportunity Commission.

Key leadership changes have also occurred—the former Chairman and about half of the FDIC's Division and Office Directors and other direct reports to the Chairman have been replaced over the past year. In addition, 26 employees have separated from the Agency specifically due to substantiated allegations of misconduct.

The FDIC has revised its anti-harassment training; centralized its harassment complaint process and relocated its discrimination complaint process to the OPC and OEEO, respectively; made enhancements at the FDIC Student Residence Center (SRC) by among other things establishing a code of conduct, increased security measures, and increased reporting requirements.

The FDIC has also updated or developed new Directives for the Anti-Harassment Program, Anti-Retaliation and Whistleblower Protection Rights, and Personal Relationships in the Workplace; improved its recordkeeping by developing an interim solution for tracking complaints and working on implementing a new case management system; and incorporated a workplace culture standard into its performance management program.

While the FDIC has made progress, as noted above, in improving its workplace culture, 5 of 30 OIG recommendations remain open and outstanding, indicating that work remains. We will continue to work with the FDIC to ensure that OIG recommendations are addressed and the FDIC continues in a positive direction with respect to improving workplace culture.

Strengthening Organizational Governance

In prior years we have found that the FDIC Divisions and Offices have worked in a siloed, independent fashion rather than addressing risks faced by the FDIC in a cohesive, enterprise-wide manner and ensuring the FDIC is able to effectively meet its mission requirements and program goals.

Fostering Agency-Wide Coordination to Work as One-FDIC

The FDIC has identified interdivisional coordination and information sharing as elevated risks in its enterprise risk management (ERM) risk profile since 2020. In FY 2025, we continued to find examples where the lack of FDIC internal coordination has impacted the FDIC's mission and functions:

- **Preparing for Large Bank Failures.** In our evaluation, *FDIC Readiness to Resolve Large Regional Banks* (December 2024), we found that FDIC Divisions did not coordinate effectively to ensure that all resolution-related systems were adequate for a large bank resolution and that existing processes for securing a failed bank's IT environment were sufficiently scalable. In addition, the FDIC had not completed an Agency-wide staffing analysis to identify the baseline level of FDIC and contractor resources that may be needed for a large regional bank resolution. We also found that the FDIC did not coordinate effectively across Divisions and Offices with key roles for large regional bank resolutions. As a result, risks to important cross-divisional program operations and mission-support functions were not highlighted, discussed, and addressed at the enterprise level.

Measuring Progress Towards Mission Goals

FDIC Board Members and senior leaders should be able to measure program goal achievement to determine if programs are on track or need adjustments to staffing, budgets, processes, or other activities. Our work has found examples where FDIC programs often lacked clear goals and metrics, or existing ones did not adequately measure program effectiveness or status.

- **Resolving Large Regional Banks.** In our report, *FDIC Readiness to Resolve Large Regional Banks* (December 2024), we found that the FDIC had processes to monitor and report on Division and Agency-level goals related to large regional bank readiness. However, these goals focused on monitoring specific activities and did not provide a comprehensive view of the FDIC's overall readiness for large bank resolutions. The FDIC had not conducted an overall readiness assessment before the failures of Silicon Valley Bank, Signature Bank, and First Republic Bank in Spring 2023. As a result, the FDIC was not as prepared as it could have been for resolving large regional banks. Improving evaluation

and monitoring, including formal tracking of corrective actions, regular testing of internal controls, and continued assessment of overall bank resolution planning will help improve the FDIC's readiness for future large regional bank resolution events.

- **Examining Bank Service Providers.** In our memorandum, *Significant Service Provider Examination Program* (SSP) (August 2025), we found that while the FDIC has established an examination framework and conducts examinations of those servicers providing core banking, payment processing, cloud service, and other technology services, it has not defined measurable program-level goals or metrics to assess overall effectiveness and efficiency of the program. As a result, we could not conclude whether the program effectively evaluates SSP risk or determines appropriate supervisory attention. We identified an opportunity to strengthen the program by clearly defining program-level goals and noted similar issues in *The FDIC's Regional Service Provider Examination Program* (RSP) (December 2023).
- **FDIC-Owned Real Estate.** In our audit, *The FDIC's Student Resident Center* (January 2026), we found that the FDIC has not determined the cost benefits or organizational risks of operating the SRC. Specifically, the FDIC could not provide documentation that SRC cost benefits have been assessed since 1986, or that organizational risks have been formally identified, assessed, or addressed. This is partly due to the FDIC's lack of asset management processes and procedures, centralized SRC-related data, and performance goals and objectives for SRC operations.

Effective governance enables the FDIC to coordinate roles, responsibilities, and actions across its Divisions and Offices. Developing clear metrics helps the FDIC Board of Directors and senior leaders assess progress toward program and mission goals and prevent wasteful spending of the DIF.

During FY 2025, the FDIC made considerable progress in addressing findings and took corrective actions to close several recommendations in this area. These actions included strengthening coordination and collaboration across Divisions for resolution readiness and during major business process changes. The FDIC also improved its ability to measure progress towards goals by closing recommendations to enhance the effectiveness of programs such as for Regional Service Providers and InTREx. Additionally, the FDIC developed performance measures to assess threat and vulnerability information sharing with financial institutions.

Sustaining Readiness to Execute Resolution and Receivership Responsibilities

The FDIC insures deposits in the nation's financial institutions and is responsible for the supervision and examination of state-chartered banks and thrifts that are not members of the Federal Reserve System for safety and soundness and consumer protection. The FDIC also resolves failed banks, conducts resolution planning for large and complex institutions, and manages receiverships.

As of September 30, 2025, the FDIC insured an estimated $10.66 trillion in domestic deposits in 4,379 institutions, of which the FDIC supervised 2,772. The DIF balance totaled $150.1 billion. Active receiverships totaled 44, with assets in liquidation of about $24.99 billion.

Following the 2023 failures of large regional banks—Silicon Valley Bank, Signature Bank of New York, and First Republic Bank—we initiated a series of reviews to assess the adequacy of the FDIC's resolution readiness and response to those failures. In FY 2025, we reported on the FDIC's preparedness to resolve large regional banks and its approach to procuring resolution and receivership services. As described below, we found that certain aspects of the FDIC's readiness efforts require further improvements to minimize losses to bank customers and the DIF, and potential costs incurred by insured depository institutions. Also, as noted in our prior assessment of Top Management and Performance Challenges, with regard to the FDIC's Orderly Liquidation Authority (OLA), we reported that the FDIC had not fully defined individual practitioner-level roles and responsibilities related to an OLA resolution.[4] Failures may occur quickly, not allowing the FDIC to fully define, assign, and train personnel for resolution tasks.

Improving Readiness for Large Regional Bank Failures

In our report, *FDIC Readiness to Resolve Large Regional Banks* (December 2024), we found that the FDIC's readiness to resolve large regional banks was insufficient to ensure an efficient crisis response. The FDIC monitored specific readiness activities but did not assess its overall readiness for such resolutions. Specifically, CISR and DRR staff identified 15 major technology gaps, including inadequate scalability of IT processes for large bank failures. Before the 2023 failures, the FDIC did not address these gaps, instead it relied on the failed banks' systems and staff to mitigate some issues. The report also noted missing elements in resolution procedures, such as the absence of a receivership expense model and a method for estimating bridge bank resolution costs. CISR's procedures did not clearly define key resolution roles used during the 2023 failures. Additionally, CISR has consistently operated below authorized staffing levels, and

[4] FDIC OIG, *The FDIC's Orderly Liquidation Authority* (EVAL-23-004) (September 2023). As of February 15, 2026, 4 of 17 recommendations to improve key elements for executing the FDIC's OLA responsibilities remained open.

the FDIC has not ensured that CISR can obtain or retain the necessary human resources to meet its objectives, nor has it adjusted processes to require fewer staff.

Procurement of Resolution of Receivership Services

In our report, *The FDIC's Procurement of Resolution and Receivership Services* (June 2025), we found that the FDIC's procurement of financial advisory and consulting services under Receivership Basic Ordering Agreements was inadequate to address potential future failures or crises. Key deficiencies included too few identified contractors, no upfront pricing framework, no emergency acquisition response team, and weak documentation and testing of emergency procurement processes.

The FDIC must remain prepared to execute all aspects of its resolution and receivership powers to maintain financial stability, even as it restructures staffing and processes. Emergency preparedness to procure the services needed to resolve unexpected financial institution failures and systemic financial risks is key to the FDIC's mission of maintaining stability and public confidence in the U.S. financial system. Improving the FDIC's emergency acquisition procedures will enhance the FDIC's ability to procure critical services during an emergency and to facilitate resolutions in the most effective manner.

Ensuring Effective Supervision

The FDIC serves as the primary federal regulator for 2,772 of the 4,379 insured depository institutions nationwide (as of September 30, 2025). The FDIC examines banks using a risk-focused approach to assess safety and soundness and consumer protection, Community Reinvestment Act performance, and adherence to laws and regulations. FDIC examinations are essential for maintaining public confidence in the banking system and protecting the DIF. By accurately identifying risks, the FDIC formulates corrective measures for individual institutions and develops broader supervisory strategies. Beyond conducting examinations, the FDIC—either independently or in collaboration with other federal regulators—issues guidance on safety, soundness, and consumer protection, with particular attention to emerging issues and technologies.

During the financial crisis of 2008-2011, FDIC examiners often identified weak risk management practices at financial institutions but delayed taking supervisory action until the institution's capital declined. Taking supervisory action after a bank's capital has declined is often too late, because financial decline tends to lead to bank failures and losses to the DIF. To avoid that result, the FDIC implemented a forward-looking supervisory initiative to identify and assess risks before they impact a bank's financial condition and to ensure early risk mitigation. These risks are ever-changing. Currently, to address identified risks, the FDIC continues to take steps to reform its supervisory processes.

Today, artificial intelligence (AI) technology is evolving and presents both opportunities and risks. In banking, AI can serve to enhance automation, fraud detection, and customer service; reduce costs and compliance risks; and aid in data-driven decision making. To mitigate potential risks, appropriate risk management frameworks and practices that are commensurate with the use, materiality, complexity, and sophistication of AI are essential. Some banks are engaged or interested in engaging in various crypto-related activities. On July 14, 2025, the FDIC, OCC, and the Federal Reserve issued a joint statement to provide clarity on banks' engagement in crypto-asset-related activities.[5] The statement highlights for banks potential risk-management considerations related to holding crypto-assets on their customers' behalf, or crypto-asset "safekeeping." The joint statement reminds banks that provide or are considering providing safekeeping of such assets that they must do so in a safe and sound manner and in compliance with applicable laws and regulations.

[5] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Joint Statement on Crypto-Asset Safekeeping by Banking Organizations* (July 2025).

Escalating Supervisory Actions

Section 38 of the Federal Deposit Insurance (FDI) Act requires that the Inspector General of the appropriate federal banking agency conduct a review and issue a written report when there is a material loss to the DIF related to an insured depository institution for which the FDIC is appointed receiver. In FY 2025, we conducted a material loss review of a large regional bank failure, Republic First Bank (described below). Similar to the *Material Loss Review of First Republic Bank* (November 2023), we reported that FDIC examiners identified risks at the bank but did not take supervisory action consistent with effective supervision practices.

- In our report, *Material Loss Review of Republic First Bank* (November 2024), we found that the direct cause of the bank's failure was its inability to hold its held-to-maturity debt securities to maturity, requiring the securities to be reclassified as available-for-sale. The unrealized losses were disclosed to the public but were not required to be fully reflected in the Republic First Bank's balance sheet and therefore were not reflected in the bank's capital ratios. Once the losses were fully recognized, all of the bank's capital ratios immediately fell below zero and the bank was closed. The FDIC was aware of the risk associated with unrealized losses at Republic First Bank and within the broader banking industry. In the First Republic Bank report mentioned above, we issued a recommendation for the FDIC to engage with other federal regulators to evaluate the need to identify noncapital triggers that would require early and forceful regulatory actions tied to unsafe banking practices before they impair capital. In 2026, the FDIC proposed rules to address noncapital or capital deficiencies.
- In the report, *Bank Supervision: Federal Reserve and FDIC Should Address Weaknesses in Their Process for Escalating Supervisory Concerns* (November 2024), the Government Accountability Office (GAO) identified weaknesses in the FDIC's procedures to escalate supervisory concerns. The GAO found that the FDIC did not have a centralized system to track recommendations for supervisory actions, limiting its ability to identify emerging risks across its supervised banks. Additionally, unlike other banking regulators, the FDIC does not have vetting meetings "to ensure that large bank examination teams and relevant stakeholders are consulted before making changes or decisions, such as escalation decisions." The FDIC also does not require large bank case managers to rotate to other banks after a few years, a practice that GAO noted helps ensure supervisory independence. According to the FDIC, it has taken steps to address GAO's findings where appropriate.

Prompt supervisory action on identified risks enables the FDIC to better safeguard the DIF and maintain public trust in the banking system.

Supervision of Third-Party Service Providers

Under the Bank Service Company Act of 1962, the FDIC, the Federal Reserve Board, and the OCC have the statutory authority to examine covered services provided by technology service providers to their regulated financial institutions. The FDIC conducts service provider examinations to evaluate the overall risk exposure and risk management performance and determine the degree of supervisory attention needed to ensure weaknesses are addressed and risks are properly managed by financial institutions using service providers.

The FDIC performs these examinations using two risk designations: SSP and RSP. SSPs are large and complex service providers designated as agreed upon by the Federal Banking Agencies for special monitoring and collaborative interagency supervision at the national level. In contrast, RSPs are smaller in size, less complex, and collaboration occurs at the regional, district or supervisory offices of the Federal Banking Agencies.

Examining Bank Service Providers. In our memorandum, *Significant Service Provider Examination Program* (August 2025), we found that while the FDIC has established an examination framework and conducts examinations, it has not defined measurable program-level goals or metrics to assess overall effectiveness and efficiency of the program. As a result, we could not conclude whether the program effectively evaluates SSP risk or determines appropriate supervisory attention. We identified an opportunity to strengthen the program by clearly defining program-level goals and noted similar issues, as we mentioned earlier, in *The FDIC's Regional Service Provider Examination Program* (December 2023).

Specifically, the OIG recommended the Director of the Division of Risk Management Supervision complete efforts to develop and implement program-level goals and metrics for both the RSP and SSP Examination Programs. The FDIC concurred with our recommendation and will complete efforts to develop and implement performance goals and metrics for the RSP and SSP Examination Programs. These efforts should help ensure more robust supervision of the risk to the FDIC presented by technology service providers.

Reforming the FDIC's Supervisory Framework

During 2025 and continuing into 2026, the FDIC has taken several steps to reform its supervisory framework. For example, the FDIC revised its supervisory framework to focus on material financial risks rather than administrative compliance.[6] The joint proposal issued by the OCC and FDIC established a definition of "unsafe or unsound practices"[7] and included guidance on when examiners can take formal early action; narrowing the definition and updating processes suggests that regulators aim to address genuine threats to insolvency—capital depletion or

[6] The Honorable Travis Hill, Nomination Hearing, 119th Cong. (2025) (*Opening Statement of Travis Hill*).
[7] *Unsafe or Unsound Practices, Matters Requiring Attention*, 90 Fed. Reg. 48835 (October 30, 2025).

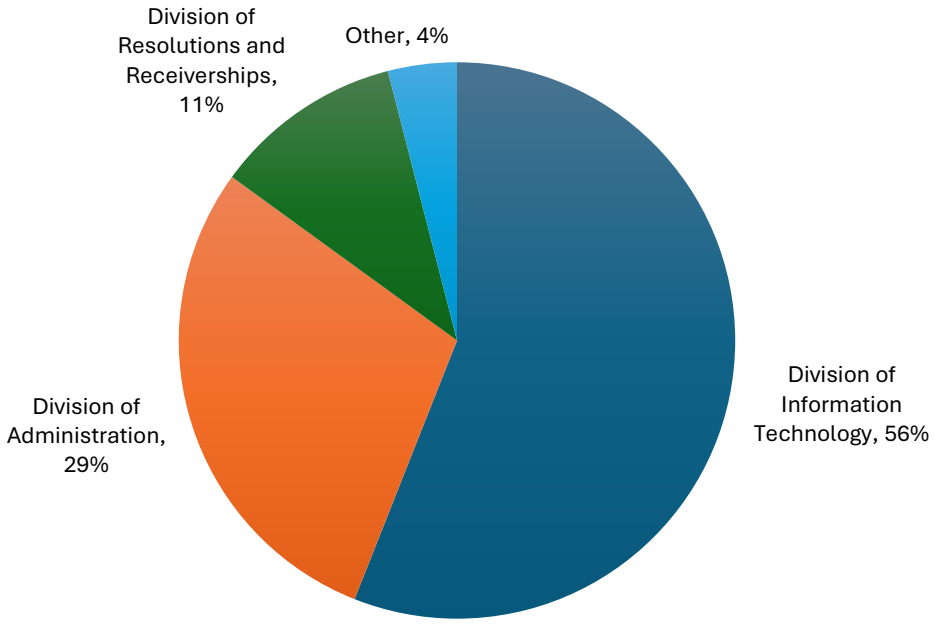
liquidity crises versus procedural issues. Also, the FDIC and the OCC issued the notice of a proposed rulemaking that would codify the removal of reputation risk from their supervisory program. The supervisory framework reforms are in their early stages of implementation, and their long-term impact remains to be seen.

Effective supervision of FDIC institutions for compliance with safety, soundness, financial crimes, sanctions risk, and consumer protection requirements is essential for maintaining public confidence in the banking system and protecting the DIF. Identifying emerging risks from new technologies, new banking practices, or changed economic conditions is critical to ensuring that the FDIC supervisory framework evolves to match changes in the financial sector.

Improving Contract Management

The FDI Act authorizes the FDIC to acquire goods and services necessary to achieve its mission. Between January 1, 2020 and December 31, 2025, the FDIC awarded 1,831 contract actions totaling more than $4.7 billion. The figure below shows how these contracts are distributed throughout the FDIC. Contract management remains a top management challenge. Our work continues to highlight the need for stronger contracting controls and a culture that prioritizes compliance with internal controls and processes.

Percent of Active Contracts ($) by FDIC Division/Office



Source: Division of Administration, Acquisition Services Branch

Adhering to Contracting Requirements and Internal Controls

In previous reports, we have identified shortcomings in the FDIC's contract management and internal control processes. These deficiencies have led to overpayments, unauthorized contractual commitments, and the abandonment of a systems contract after incurring nearly $10 million in costs. The significance and pervasiveness of these issues underscore the need for continued FDIC-wide emphasis on compliance with internal controls and responsible stewardship of operating costs incurred by the DIF. Through our audit of the procurement of resolution and receivership services, for example, we found that strengthening emergency acquisition procedures will improve the FDIC's ability to procure critical services during emergencies and support effective resolutions.

In our more recent audit of the FDIC's *Oversight of the Infrastructure Support Services Contract* (January 2026), we examined the FDIC's oversight of a $300 million Basic Ordering Agreement to provide day-to-day information technology operational support for its infrastructure facilities, hardware, software, and systems and identified contract oversight weaknesses. We reported that while the FDIC had made progress in addressing the weaknesses we identified during the audit, oversight of the contract was not effective in ensuring that key contract personnel and the Contractor complied with internal policies and procedures or the infrastructure support services contract terms and conditions. We noted weaknesses in service level metric monitoring, review and approval of contractor invoices, and practices for protecting data and ensuring timely completion of role-based training for contractor personnel. The audit also found funds to be put to better use for service level credits due and questioned costs resulting from missing data to support contract invoices.

Improving Procurement of Services

In our report, *The FDIC's Procurement of Resolution and Receivership Services* (June 2025), we found that the FDIC's procurement of financial advisory and consulting services under Receivership Basic Ordering Agreements (RBOA) is inadequate to address potential future failures and crises. We identified several critical deficiencies:

- An insufficient number of contractors with RBOAs,
- Lack of an upfront pricing framework,
- Absence of an emergency response acquisition team,
- Lack of the development and implementation of emergency acquisition procedures,
- Weak documentation analysis and establishment of documented deliverables, and
- Non-performance of retrospective reviews of the FDIC's implementation of emergency acquisition procedures and lack of training and guidance to Division of Complex Institution Supervision and Resolution Executive Management and employees.

These contracting-related gaps leave the FDIC vulnerable during times of crisis and hinder its ability to respond effectively. Effective contracting is essential for both routine operations and crisis response. The FDIC should have appropriate processes and internal controls to ensure it receives the goods and services it contracts for, and that agency employees consistently adhere to these controls and processes. By improving its emergency acquisition procedures, the FDIC will be better equipped to procure critical services during emergencies and facilitate resolutions efficiently, ultimately reducing operating expenditures for the DIF.

During FY 2025, the FDIC made progress in addressing prior procurement-related findings, closing several recommendations—including those to address the potential for conflicts of interest, contract portfolio reporting, and other contract oversight issues, as identified in our

work.[8] Still, with the high number of contract actions and their significant dollar value, vigilant oversight and strong internal controls are critical to ensure that the FDIC receives the goods and services it contracts for and that FDIC employees follow these processes and implement appropriate controls to reduce DIF operating expenses.

[8] FDIC OIG, *Conflicts of Interest in the Acquisition Process* (EVAL-24-06) (September 2024) and FDIC OIG, *Contract Oversight Management* (EVAL-20-01) (October 2019).

Enhancing Cyber and Data Security

Effective cybersecurity and data security of FDIC systems is critical to all aspects of the FDIC's mission and goals, especially during a crisis. FDIC systems contain sensitive information, such as personally identifiable information on FDIC employees and contractors; bank account information for millions of depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data. Further, certain FDIC systems interconnect with bank systems to receive information for examinations, quarterly Call Report data, and information from failing banks. Although the FDIC's Office of the Chief Information Security Officer has primary responsibility for leading the FDIC's information security and privacy programs, the Division of Information Technology plays a critical role in implementing security and privacy controls in the operational IT environment, and all FDIC employees and contractors have responsibility for security.

Cybersecurity and data security remain management challenges for the FDIC. Our assessments show that while the FDIC implemented an effective information security program in FY 2025, operational inconsistencies remain. We have identified areas where the FDIC can further improve its IT systems' control posture and issued recommendations to address ongoing access vulnerabilities, cloud security gaps, and scalability concerns. These steps will help ensure systems can meet both ongoing mission execution and elevated operation demands during periods of stress and crisis.

- **Information Security Program.** In *The FDIC's Information Security Program—2025* (September 2025), the report concluded that the FDIC achieved a Maturity Level 4 ("Managed and Measurable") under the FY 2025 Federal Information Security Modernization Act of 2014 metrics, indicating an effective program with several controls and practices that meet requirements. However, the evaluation identified notable internal control weaknesses that diminish certain aspects of the program. The FDIC did not implement privileged access review frequency requirements for both systems tested in the review, and the FDIC used an incomplete and inaccurate user recertification listing for one tested system.
- **Cloud Security Controls.** Our third cloud-related report, *Audit of Security Controls for a Cloud Platform and Application* (September 2025), evaluated the security controls of a fifth cloud platform and its application. The audit covered nine critical IT security demands through policy review, testing, interviews, and penetration testing. Two primary security deficiencies were identified in Identity and Access Management and Protection of Cloud Secrets. Seven technical weaknesses were also identified in Insecure Coding Practices and Cloud Service Provider vulnerabilities, with the latter requiring remediation by the provider. The audit found that the FDIC needs to further strengthen

its cloud security practices, focusing on identity and access management, data protection, and secure coding. Misconfigured controls could expose systems and data to malicious exploitation.

- **Information Technology Scalability.** Our report, *FDIC Readiness to Resolve Large Regional Banks* (December 2024), identified 15 significant technology and security gaps in the resolution of large banks, driven by the size and complexity of these resolutions. As noted earlier in our discussion of Coordination to Operate as One FDIC, DRR and CISR did not sufficiently coordinate the technology gaps they identified with the Chief Information Officer Organization, resulting in inadequate assurance that all resolution-related systems could support a large bank resolution. The FDIC's September 2025 ERM Risk Inventory identified Resolution Technology at an elevated risk level with significant potential impact. It is paramount for the FDIC to continue to ensure the availability, confidentiality, integrity, and scalability of FDIC systems and data for its day-to-day mission and during crises.

During FY 2025, the FDIC made substantial progress in addressing prior IT-related findings, closing multiple recommendations—including those to remediate wireless networking vulnerabilities, implement cloud computing services, and enhance Windows Active Directory. The FDIC also resolved three FISMA-related recommendations from prior FYs 2022 and 2024.

According to the FDIC's *2024 Annual Report* (March 2025), the FDIC completed the first phase of its multi-year IT modernization initiative by migrating several mission-critical applications and services to cloud environments, aimed at reducing its primary data center footprint. The FDIC reported that it improved cloud data management and analytics, launched a Data Orchestration Platform, and advanced modernization by adopting agile and DevSecOps practices, launching Supervision 360, and planning to replace a legacy system for managing deposit insurance assessment operations and compliance. The FDIC also reported enhanced cybersecurity by implementing Zero Trust principles, updating authentication, improving identity and access management, and aligning security controls with National Institute of Standards and Technology standards and Office of Management and Budget (OMB) guidelines.

Implementing the Use of Artificial Intelligence

The control issues identified above—such as access vulnerabilities, cloud security gaps, and scalability concerns—are equally relevant as the FDIC expands its own use of AI. In September 2025, the FDIC published its AI compliance plan, which details strategies to foster AI innovation, strengthen AI governance, and build public trust in AI applications. In fostering AI innovation, the FDIC has not identified unique barriers to the responsible use of AI at the FDIC and has proactively taken steps to enhance access to the necessary software tools, open-source

libraries, and deployment and monitoring capabilities needed to rapidly develop, test, and maintain AI applications.

The FDIC maintains an AI Coordination Committee to develop, document, and share AI governance and risk management procedures; has developed an enterprise-level AI workforce development plan; and is conducting internal training in AI fundamentals for practitioners and AI enablers. In approving AI Governance, the FDIC is reviewing its internal policies on IT infrastructure, data, cybersecurity, and privacy to maintain alignment with the requirements of OMB Memorandum M-25-21, Executive Order 14179, Executive Order 13960, and applicable laws, and has created an AI Use Case Inventory. To foster public trust in federal use of AI, each Division and Office maintains an OMB-compliant template in which potential high-impact uses are documented. The FDIC is also taking steps to implement risk management practices and (per M-25-21) will monitor and address any non-compliant AI.

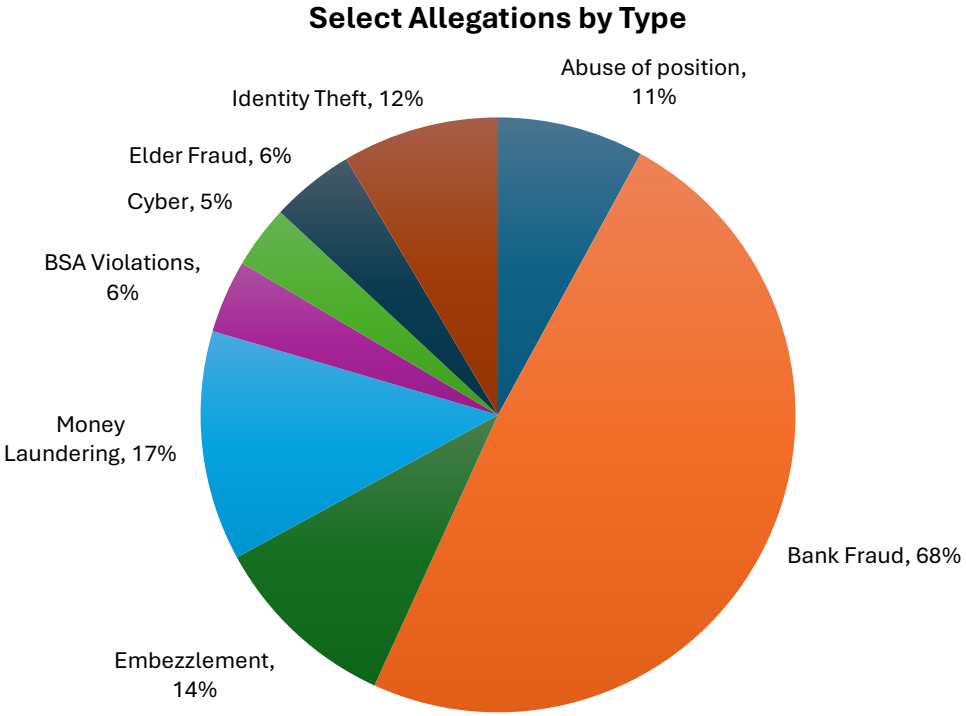
Given the sensitivity of the information that the FDIC maintains, along with the ever-evolving threats to cyber and data security, the FDIC should continue to ensure that its systems and data in the cloud or on premises are secured, control weaknesses are effectively addressed, and new technologies are prudently used to strengthen the FDIC mission. Failure to do so could result in damage to FDIC systems and data, hindering its ability to maintain stability and confidence in the nation's financial system.

Identifying and Combating External Fraud and Misrepresentation

The FDIC OIG has broad authority to investigate complex misconduct within FDIC-supervised and insured institutions, focusing on high-risk activities such as bank fraud, money laundering, embezzlement, cybercrime, currency manipulation, and Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) violations. Investigations often involve senior executives, insiders, customers/borrowers, financial professionals, and organizations including banks, FinTech firms, and international financiers. By targeting sophisticated schemes and diverse actors, the FDIC OIG protects FDIC assets, programs, and public trust. We are sharing our analysis of recent allegations of fraud so that the FDIC and the public have heightened awareness of the risks and challenges that various types of fraudulent activity can pose to institutions and consumers.

Insider Fraud

Insider fraud remains a significant risk within financial institutions. In FY 2025, we opened 127 investigations covering a wide range of allegations, including bank fraud, money laundering, embezzlement, identity theft, abuse of position, elder fraud, Bank Secrecy Act (BSA) violations, and cyber-related offenses. Bank fraud emerged as the most common issue, with both financial institution (FI) employees and executive managers implicated. See the chart below depicting select allegations by type.



Source: OIG Office of Investigations' Case Management System

Our analysis of FY 2025 open case data shows that both FI employees and executive management are frequently implicated in a variety of fraud types, including abuse of position, embezzlement, money laundering, and identity theft cases. These findings highlight the need for continued monitoring and robust internal controls at all FI organizational levels. Embezzlement cases showed a clear pattern, as employees were involved more often than executive managers, suggesting weaknesses in internal controls, including poor segregation of duties, excessive delegation of authority, and inadequate oversight. Similarly, abuse of position was primarily associated with employees, while executive managers were also involved, to a lesser extent. Money laundering, BSA violations, cyber-related offenses, elder fraud, and identity theft were also investigated, with employees generally more frequently implicated than executive managers. While our analysis focused on internal FI actors, it is important to note that the involvement of FI customers in fraud cases is also high, especially in categories such as bank fraud and money laundering. This observation highlights, along with insider threats, external risks from customers remain a significant concern for financial institutions. See the table below for more details.

Allegations by Financial Institution Personnel and Customers

Allegation Type	Count*	FI Employee	FI Executive Manager	FI Personnel	FI Customer
Abuse of Position	14	8 (57%)	3 (21%)	11 (79%)	0 (0%)
Bank Fraud	86	38 (47%)	8 (9%)	46 (53%)	37 (43%)
Embezzlement	18	13 (72%)	4 (22%)	17 (94%)	3 (17%)
Money Laundering	22	6 (27%)	0 (0%)	6 (27%)	17 (77%)
BSA Violations	7	3 (43%)	1 (14%)	4 (57%)	5 (71%)
Cyber-related	6	2 (33%)	0 (0%)	2 (33%)	0 (0%)
Elder Fraud	8	5 (63%)	0 (0%)	5 (63%)	2 (25%)
Identity Theft	15	7 (47%)	1 (7%)	8 (53%)	7 (47%)

*The count is the frequency of occurrence of allegation type. The total allegation count is greater than the open investigations as a single case may involve multiple allegations.

Source: OIG Office of Investigations' Case Management System

Our investigative work consistently demonstrates that fraud and misconduct most often involve those entrusted with institutional operations. While the FDIC has a robust infrastructure and has allocated significant resources to investigate and pursue FI insiders who engage in wrongdoing, often partnering with the OIG, this pattern highlights a critical area of ongoing risk. By continuing to recognize the prevalence of insider involvement, the FDIC can prioritize enhanced oversight of fraud in its examination process, including review of internal control frameworks and proactive engagement with institutions. Addressing these challenges is essential not only for strengthening institutional resilience and accountability but also

protecting consumers and maintaining public confidence in the integrity of the U.S. financial system.

Scams Targeting Unwitting Consumers

As we noted in our prior TMPC report, scams targeting consumers continue to rise and grow increasingly sophisticated. The FDIC OIG continues to receive reports of the four most common types of schemes: relationship scams, investment scams, government impersonation scams, and business email compromise scams. In relationship scams, a fraudster creates a fake online identity to gain a victim's trust and manipulate them emotionally. Investment scams involve offers of low- or no-risk investments and guaranteed returns with complex strategies to manipulate or steal from the victim. As we described last year, a "Pig Butchering" romance scheme is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally, in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the monetary investment.

We have investigated numerous government impersonation scams that often involve unsolicited phone calls, text messages, or e-mails that claim to be from the FDIC or FDIC OIG. Scammers frequently use the FDIC or the OIG's seal or logo and even names of actual employees, to make their demand for funds appear legitimate.

In cases of FDIC impersonation, scammers may contact an individual with the claim of a grant or monetary award and request personal or financial information or ask for money or gift cards. These schemes often require advance payment, which is a warning sign. According to the Federal Trade Commission's Consumer Sentinel Network Data Book, consumers reported losing over $12.5 billion to fraud in 2024, a roughly 25-percent increase over $10 billion reported in 2023. Impersonation scams accounted for nearly $2.95 billion in reported losses, resulting from 845,806 reports.[9]

For FDIC OIG impersonations, scammers may contact an individual pretending to be OIG personnel, sometimes using the names of Special Agents to lend credibility to their claims. As a scare tactic, they might inform the recipient that they are under investigation and must pay a fee or fine to avoid arrest. The fee or fine is frequently requested to be paid through gift cards, cryptocurrency, or other forms of payment.

Still another type of payment scam is known as a business email compromise scam. The scammer targets a business or individual and takes over an official account, or uses email spoofing, to attempt to redirect legitimate payments to an illicit account controlled by the scammer to steal from the victim.

[9] Federal Trade Commission, *Consumer Sentinel Network Data Book 2024* (March 2025).

According to the FBI's Internet Crime Complaint Center (IC3) 2024 Internet Crime Report, individuals reported losing $6.57 billion to investment scams and $2.77 billion to business email compromise scams in 2024. These figures stem from 47,919 complaints and 21,442 complaints, respectively.[10] The number of complaints about scams, and the amount of losses, reported to the IC3 generally grew in the past 4 years.

As an emerging type of scam, in December 2024, the FBI warned that criminals are increasingly using generative AI to commit fraud on a larger scale. Generative AI enables scammers to create convincing fraudulent content more efficiently, making schemes such as romance and investment scams harder to detect. While creating synthetic content with AI is not inherently illegal, such content can be misused to facilitate crimes like fraud and extortion.[11]

Addressing Misuse of the FDIC Name and Logo

Section 18(a)(4) of the FDI Act specifically prohibits any person from harming consumers by misusing the FDIC name or logo or making misrepresentations about deposit insurance. The FDIC may investigate any claims under this section and may issue administrative enforcement actions, including cease and desist orders, and impose civil money penalties against perpetrators.

As of December 31, 2025, the FDIC had received approximately 1,200 misrepresentation allegations through its portals, which is roughly the same number of allegations received in 2024 and a 60-percent increase from 2023. The FDIC took hundreds of actions in 2025, including initiating the takedown of approximately 360 websites that, working in partnership with other stakeholders, including the OIG, were determined to be fraudulent; making referrals to other appropriate agencies; and issuing one public cease and desist letter.

FDIC awareness of the detrimental effects of fraud occurring at insured and supervised institutions can help prevent and deter such fraud from occurring. Further, by continuing to protect consumers from fraudulent schemes and misrepresentations, the FDIC can help safeguard taxpayer savings, provide them with trusted financial products and services, and foster public confidence in the FDIC. The FDIC regularly engages in outreach to FI and consumers to help build awareness around the potential for fraud faced by both FIs and consumers. See FDIC Consumer News | FDIC.gov and Money Smart | FDIC.gov. The OIG will continue to work with the FDIC and law enforcements partners to investigate and combat fraud that undermines the integrity of the financial sector.

[10] Internet Crime Complaint Center (IC3), *Federal Bureau of Investigation Internet Crime Report 2024* (2025).
[11] IC3, *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud* (December 2024).

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.