AUSTIN BANK, JEFF AUSTIN III

Proposal and Comment Information

Title: Proposed Revisions to the Federal Reserve Policy on Payment System Risk and the Guidelines for Account and Services Requests, OP-1878

Comment ID: FR-2026-0013-01-C107

Subject

Docket Nos.: OP-1878; R-1892; R-1893

Submitter Information

Organization Name: Austin Bank

Organization Type: Company

Name: Jeff Austin III

Submitted Date: 07/27/2026

Please consider the attached comments.
Thank you.
Jeff Austin III

Jeff Austin III
Chairman of the Board
Jacksonville

P: 903.586.1526 ext. 5193
F: 903.541.2086

AUSTIN BANK

July 27, 2026

Benjamin W. McDonough Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Re: Proposed Revisions to the Federal Reserve Policy on Payment System Risk and the Guidelines for Account and Services Requests; Regulation A: Extensions of Credit by Federal Reserve Banks; and, Regulation D: Reserve Requirements of Depository Institutions (Docket Nos.: OP-1878; R-1892; R-1893)

Dear Mr. McDonough:

Thank you for the opportunity to comment on the Board of Governors of the Federal Reserve System's Request for Comment (RFC) on Proposed Revisions to the Federal Reserve Policy on Payment System Risk and the Guidelines for Account and Services Requests; Regulation A: Extensions of Credit by Federal Reserve Banks; Regulation D: Reserve Requirements of Depository Institutions.

Legal eligibility under the Federal Reserve Act is a necessary condition but is not, standing alone, sufficient for access. The Board's obligation to assess not only eligibility but also the underlying risk profile and the sufficiency of ongoing supervision is essential. The possession of a bank charter, whether state or federal, should not result in entitlement to payment account access. In several cases, potential applicants may hold charters with non-uniform standards or limited federal oversight, which increases the importance of consistent, enforceable expectations—regardless of underlying charter type.

We recommend that the Board formally condition Payment Account access on maintaining robust governance, independent risk management, internal controls, and compliance functions commensurate with the applicant's size, complexity, and activities. The Board should carefully evaluate the qualifications and experience of senior management and operational leaders responsible for payments processing, compliance, and cybersecurity. Where an applicant is entering 'new business' or scaling rapidly, the Board should consider more frequent post-implementation reviews and a conservative progression of permitted

Member FDIC

903.586.1526 Phone
903.541.2039 Fax

AustinBank.com

200 E. Commerce
P.O. Box 951
Jacksonville, TX 75766

SINC 1900

activity to validate controls in real-world conditions. The process to obtain a Master Account should remain rigorous and must remain separate from the Payment Account process. We commend the Board for maintaining that position in this RFC and recommend that it remain in the final rule. Payment Account holders that wish to obtain a Master Account should be required to submit a new application subject to the full Master Account review framework. Master Account access should remain reserved for institutions with comprehensive federal prudential supervision and federally insured deposits.

The payments system's integrity depends on robust detection and prevention of illicit finance, including money laundering, terrorist financing, and sanctions evasion. We recommend that the Board categorically condition access on a mature and demonstrably effective BSA/AML/CFT and sanctions compliance program that includes adherence to the same requirements banks are subject to: risk-based customer due diligence, customer identification programs, beneficial ownership identification, transaction monitoring, sanctions screening, investigations, suspicious activity reporting, and independent testing functions staffed by qualified personnel. Applicants and Payment Account holders must be overseen by a federal banking agency to ensure compliance with these requirements. Operational risk and cybersecurity warrant equally rigorous attention. Payment Account holders should be required to implement strong cybersecurity, information security, and data protection measures, including identity and access management, IT resilience, network and cloud security, and third-party risk management commensurate with critical payments operations.

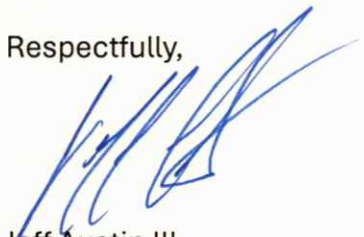
Account holders should demonstrate competence in these areas during the initial application process and on an ongoing basis thereafter and be required to report material compliance, operational, and cyber events to the Reserve Bank and the Board. Applicants and Payment Account holders must be overseen by a federal banking agency to ensure compliance with these requirements, or at a minimum be required to complete an annual audit by a qualified third-party to ensure that all regulatory requirements are met. Applicants should also maintain credible recovery and resolution plans to ensure orderly wind-down without disrupting other participants. At a minimum, entities seeking access to a Payment Account should maintain appropriate insurance coverage equal or like what bank holding companies must maintain.4 Relevant coverage could include professional liability/errors and omissions, crime or fidelity bond coverage, specie coverage for digitally native firms with cold storage exposure, cyber and privacy liability, technology errors and omissions, and general liability.

Potential applicants may engage in activities for which legislative and regulatory frameworks are evolving (including certain digital asset and stablecoin-related activities). Where fundamental supervisory and legal questions remain unresolved—such as the primary supervisory responsibility, permissible scope of activities, custodial practices, segregation requirements, and redemption rights—the Board should proceed only with heightened safeguards and retain discretion to deny or terminate access where core risks cannot be adequately managed.

And lastly, the Board should articulate, in advance, the enforcement tools it will use to respond to deficiencies, including the ability to impose additional conditions, restrict activity, or terminate access. The Board should make clear that Payment Account access is a privilege that can be withdrawn if an accountholder fails to meet operational, risk management, or compliance expectations. Applicants should maintain credible recovery and resolution strategies proportional to their activity level and interconnectedness, with periodic testing to validate feasibility.

I appreciate this opportunity and am available for any questions or concern. My office number is 903-541-2093.

Respectfully,



Jeff Austin III
Chairman