November 9, 2026

Mr. Eric S. Slee
Assistant Secretary of State, Securities Division
Office of the Mississippi Secretary of State
P.O. Box 136
Jackson, MS 39205-0136

Submitted via electronic mail to reed.inmon@sos.ms.gov

Re: Proposed Amendments to Mississippi Securities Act Rule 6.25(EE) – Accessing a Client's Account

Dear Mr. Slee:

The Financial Data and Technology Association of North America ("FDATA") appreciates the opportunity to comment on the Securities Division's ("Division") proposed amendments to Rule 6.25(EE) of the Mississippi Securities Act Rules, which governs investment adviser access to client accounts. FDATA commends the Division for proactively updating the rule to reflect the technical reality of modern open banking technology and the clear demand among investors and their advisers to securely connect their accounts to more effectively manage their finances.

FDATA is the leading trade association advocating for consumer, small business, and investor data rights in financial services across North America. Founded in 2018, our members are financial technology firms whose products and services collectively serve more than 100 million consumers and small businesses across the United States. While the specific use cases our members provide vary widely from tools that help consumers manage their budgets to platforms that support more robust retirements, all of our members' services are built on one core capability: the ability of individuals to permission access to their own financial data held by other institutions.

FDATA has engaged extensively and productively with state securities regulators on this precise issue. In February 2025, we wrote to the North American Securities Administrators Association ("NASAA") urging that its 2019 Account Access Model Rule and FAQs be revisited in light of regulatory and technological developments. FDATA has since participated throughout the Ohio Division of Securities' rulemaking on credential-based account access and, in February 2025 and July 2026, commented on Missouri's proposed account access rules. The Division's proposal reflects many of the lessons of those proceedings, and FDATA is broadly supportive of it. We respectfully offer two targeted clarifications to ensure the rule operates as the Division intends.

The Proposal Appropriately Modernizes Mississippi's Approach to Client-Permissioned Access

FDATA strongly supports the Division's decision to repeal the requirement that a data aggregation software company maintain an agreement with the custodian or online account platform as a condition of permissible access. In open finance, an individual's right to access and share their own financial data should never depend on the commercial consent of the incumbent institution holding that data. As FDATA explained in our letter to NASAA, this condition is out of step with federal policy: the Consumer Financial Protection Bureau's ("CFPB") 2024 rule implementing

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act") specified that data aggregation platforms do not need agreements with financial institutions to facilitate consumer-permissioned access. And as FDATA described to the Ohio Division of Securities, members that have sought such agreements with custodians have too often been turned away outright or presented with terms so onerous as to amount to an insurmountable barrier to data access. Removing it places the decision right where it belongs: with the investor, who should have the choice to determine whether to grant their adviser access to their financial data.

The Proposal Aligns Mississippi with National Standards

Financial data portability is a statutory federal right under Section 1033 of the Dodd-Frank Act. While the CFPB's implementing rule is the subject of continued rulemaking and litigation, the underlying right remains, and consumer expectations of secure, permissioned data sharing have only strengthened. Trump Administration policy points in the same direction. Executive Order 14405, *Integrating Financial Technology Innovation Into Regulatory Frameworks*, directs federal financial regulators to "remove overly burdensome and fragmented regulations and supervisory practices that form barriers to entry" for financial technology firms, and Executive Order 14330, *Democratizing Access to Alternative Assets for 401(k) Investors*, directs regulators to remove burdens that impede American workers' ability to grow their retirement savings.

These considerations are especially acute for retirement savers. For many Mississippi households, a workplace retirement account is their largest financial asset, yet the employer, not the investor, selects the plan's custodian. If advisers cannot use secure, client-authorized technology to manage these held-away accounts, investors may lose professional oversight of the accounts that matter most or be steered toward whatever advice the incumbent chooses to sell. As FDATA has long cautioned, such restrictions risk a two-tiered framework in which investors have fewer rights at the state level than federal policy affords them. By supporting investor choice, the Division's proposal sensibly avoids that outcome.

The Custodian Interference Standard Should Be Anchored in Applicable Law, Not "Reasonableness"

Proposed subsection (EE)(1) conditions permissible access on such access not interfering with the custodian's ability "to enforce reasonable antifraud, data privacy and protection, and cybersecurity measures in compliance with applicable federal and state laws, regulations, and guidelines." This language is identical to a provision of Ohio's proposed rule on which FDATA has commented, and our concerns apply equally here.

"Reasonable" is one of the most elastic terms in legal usage. Applied to a custodian's security and privacy practices, it is a standard the custodian itself will define, document in its own policies, and invoke at its own discretion. Without a clear definition of "reasonableness" from the regulator, each custodian may take a different view, leaving advisers uncertain whether their tools comply. A custodian could deem any non-application programming interface ("API") access method "unreasonable" even where it offers independent providers no alternative, or treat any provider absent from its approved vendor list as an unreasonable privacy risk. Such determinations often function in practice as market access decisions that may further anticompetitive intent, even where they are styled as security judgments.

Moreover, the reference to "guidelines," which do not carry the force of law, compounds the problem. Nor is litigation a realistic check: small and mid-sized fintech companies are rarely positioned to sue the large custodians on which they depend for data access. In practice, custodian invocations of this standard are likely to go unchallenged not because they are applied correctly, but because the power imbalance makes challenge impractical.

To address this issue, FDATA notes that Mississippi could refer more explicitly to existing law. Federal and state law already impose robust antifraud, data privacy, and cybersecurity obligations on custodians. FDATA recommends that subsection (EE) (1) be tied strictly to those existing obligations, for example:

> 1. The access does not interfere with the account custodian's ability to comply with antifraud, data privacy and protection, and cybersecurity requirements imposed by applicable federal and state laws and regulations;

Alternatively, the Division should require a custodian invoking this provision to demonstrate, through documented, objective criteria, that the specific access presents a genuine and identifiable risk, that it applies the same criteria to all similarly situated providers, and that no less restrictive means are available.

The Liability Provision Should Be Limited to Security Breaches and Data Misuse

Proposed subsection (EE)(2)(ii) prohibits advisers from disclaiming responsibility for "any data breaches, data misuse, or other client harm" caused by use of the client's identifying information by the adviser, its personnel, or its third-party technology provider. FDATA supports clear accountability for security failures, but "other client harm" is undefined, leaving advisers uncertain what harm triggers liability and who is responsible when issues arise. Read broadly, it could expose advisers and their technology providers to claims arising from routine market movements or from technical failures on the custodian's side, discouraging advisers from using secure, client-authorized tools at all. FDATA recommends that the Division strike "or other client harm" or, alternatively, clarify that the provision reaches only losses directly caused by a security breach or misuse of client data, and not market losses or technical failures attributable to the custodian.

Conclusion

FDATA remains committed to consumer data rights, privacy, and secure data portability, and commends the Division for advancing a framework that protects Mississippi investors while preserving their ability to work with the advisers and tools of their choosing. We would be pleased to serve as a technical resource to the Division on open banking architecture, API standards, and authentication frameworks, and are available to meet with Division staff at any time.

Sincerely,

Steven Boms
Executive Director
FDATA