SIFMA Data Aggregation Principles

Data aggregation applications compile customer financial information from multiple accounts and institutions onto a single platform. These applications may help investors better understand their overall financial situation and make more informed investment and financial decisions while, at the same time, create security risks for the financial institutions' data systems and individual investor information. SIFMA has adopted these principles as guidance for our members when working with data aggregation applications. While each member must determine for itself whether and how best to address these issues, these principles strive to provide customers with secure access to their financial information, while maintaining the security and integrity of our members' systems.

1. Access

- Customers may use third-parties to access their financial account data and SIFMA member firms believe that such access should be safe and secure.

2. Security and Responsibility

- Customers should not have to share their confidential financial account credentials (personal IDs and passwords) with third-parties.
- Customers deserve assurances that anyone accessing their financial account data will keep it safe and secure, adopt the same data and security standards followed by regulated financial institutions, and take full responsibility for any data that they receive and provide to others.

3. Transparency and Permission

- Customers should first receive a clear and conspicuous explanation of how third parties will access and use their financial account data, and then be able to consent affirmatively to this activity before it begins.
- Customers should be able to withdraw their consent easily and at any time with confidence that third parties will delete and stop collecting their financial account data and delete any access credentials or tokens.

4. Scope of Access and Use

- Customer information available to share with third parties typically includes financial account data such as holdings, balances, and transaction information, and does not include other non-public and confidential personal information.
- For customer protection, account activities such as third-party trading, money or asset movement, client verification, and other services that go beyond financial account data aggregation should be subject to separate agreements and require separate informed affirmative consent.