FDATA North America Privacy Principles- High-Level Overview

March 2023

- **Data types:** Critical to the success of any privacy framework is the application of a risk-based approach for data governance; in other words not all data is created equal. This requires the delineation of data based on how it is collected, processed, and utilized. In the context of customer-permissioned data access, FDATA recognizes four key categories of data: User-directed, proprietary, derived, and anonymous.
- **Data minimization** Data minimization is fundamental to the trust and agreement between customers and third parties. FDATA North America strongly supports a legally binding requirement that data holders must provide to their customer the right to access and share access to non-proprietary data elements that are available to them today, either online or in print. While data providers should not be permitted to determine whether a third party can access customer-permissioned data, third parties should not collect more data than that which has been authorized by the customer and which are necessary to fulfill the use case for which the customer has opted in to.
- **Secondary Use:** FDATA supports strong, risk-based protections around secondary uses of customer data by third parties. To ensure product and credit model enhancements, economic research, and other important use cases, we offer that it is important to allow for secondary usage of previously permissioned data that has been subsequently de-identified.
- **Liability:** FDATA has long advocated that the entity responsible for a data preach that results in financial loss is the entity that is responsible for making that consumer or small business whole, and it is the responsibility of an entity that has suffered a data breach to notify impacted end users, either directly or though a service provider.
- **Oversight:** FDATA supports a regulatory regime in which federal prudential regulators are responsible for overseeing the relationships between insured depository institutions and third-party data aggregators. In the US, the Consumer Financial Protection Bureau (CFPB) should be responsible for supervising customer-permissioned data aggregators. This would provide the uniformity and certainty necessary to foster a safe and competitive marketplace.
- **Technology:** To the extent credential-based authentication is utilized for authenticating an end user, FDATA North America believes that the data aggregator or third party should only retain an end user's credentials for as long as necessary to deliver the product, tool, or service for which the end user has opted in to as an extension of data minimization principles.
- **Authorization**: data providers may not override an end user's authorization to share data with an accredited third party.