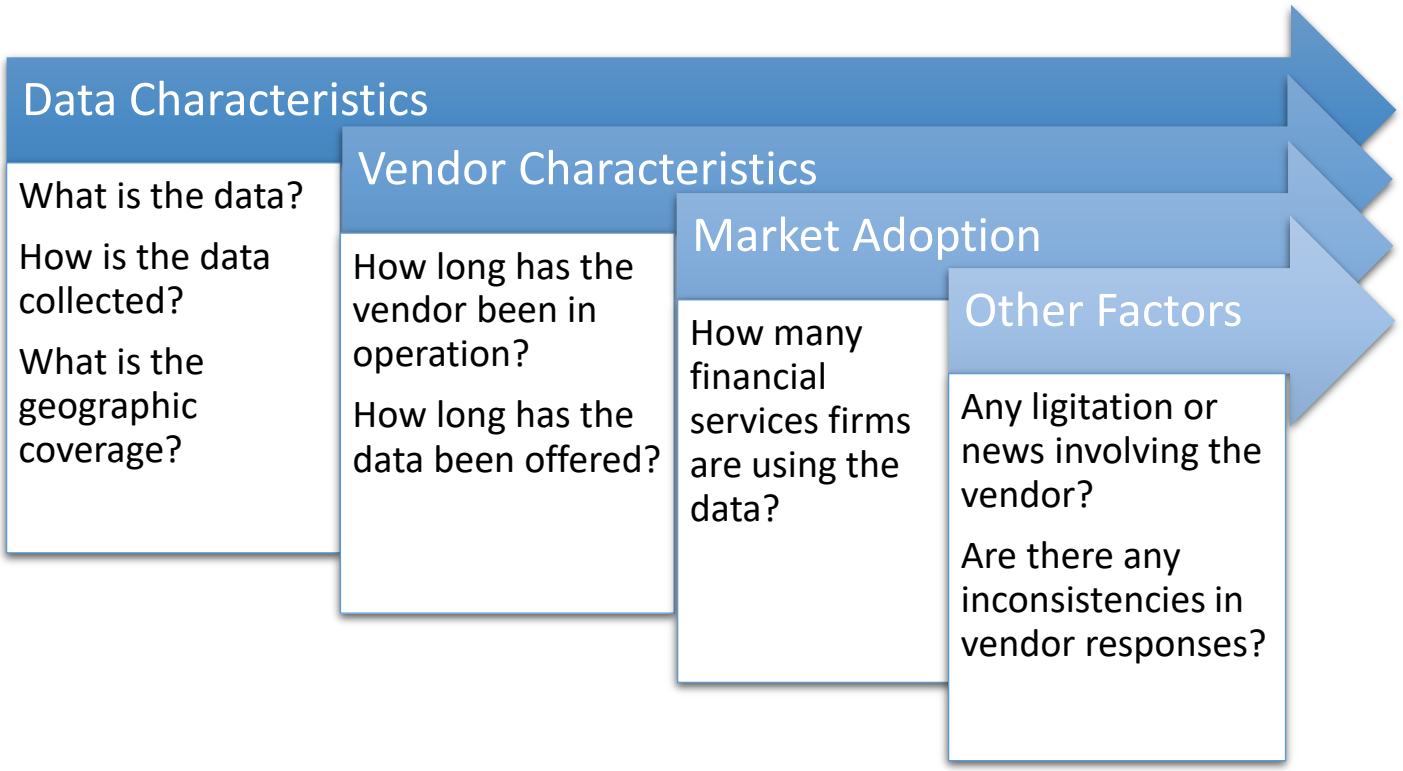
Alternative Data Identification Factors

"Alternative data" refers to non-traditional datasets that investors use to guide their investment strategy. In the financial services industry, there is no agreed-upon definition of the term. To address this issue, FISD has developed the following risk-based factors to assist financial services firms in identifying Alternative Data and, if necessary, subject such information to further due diligence review. It's important to note that no single factor below is dispositive in designating a particular dataset as Alternative Data. Similarly, a potentially concerning issue with one factor may be resolved when looking at other factors. Financial services firms should consider the totality of the circumstances in making their Alternative Data designations and may include additional factors and choose how to weigh those factors according to their specific requirements.



LEGAL REVIEW & DUE DILIGENCE

Based on the information generated from the factors, each firm may set its own standards on what to classify as Alternative Data, which may require further legal review

Below are additional details about the factors that may be used by legal, compliance, or data professionals of the data buying firm ("Firm") to identify and review Alternative Data for investment-related purposes.

Data Characteristics: What type of data is at issue? How is it collected and transformed prior to Firms' receipt of the information?	In order to assess and mitigate the risks associated with a particular dataset, Firms often seek to understand the data category at issue and the vendor's data collection and transformation practices. For instance, geolocation information as a data category may have inherent privacy risks to consider; whereas pricing data may appear to pose low risk, but additional questions may be warranted if the vendor is collecting the information via web scraping, to confirm the vendor's adherence to industry norms (see FISD's Web Data Collection Consideration). As such, Firms may consider utilizing a list of Alternative Data categories. They may create a list themselves or utilize a third party resource, such as FISD's Guide to Alternative Data. Given the variety and evolving nature of the data ecosystem, Firms may consider updating their Alternative Data category lists periodically from time to time. For Firms developing their own lists of Alternative Data categories, questions and factors to consider include: • **What categories of data present higher potential risk?** In answering this question, Firms may take different approaches including, but not limited to, i) drawing on their experiences; ii) consulting with outside counsel; and iii) reviewing lists of Alternative Data categories published by FISD, Neudata, Eagle Alpha, and AlternativeData.org. • **What data collection methodologies present higher potential risk?** As noted, even an innocuous-seeming dataset may have heightened risk implications if the data is gathered using processes (e.g., web scraping) or technology (e.g., drones, mobile apps) that are indicative of potential Alternative Data. • **What is the underlying subject and/or geographic coverage of the data?** Firms may choose to engage in additional due diligence if the data: i) implicates privacy concerns (e.g., people migration patterns, spending habits); ii) is sourced from sectors that are not generally in the public domain (e.g., healthcare stats); or iii) emanate from restrictive jurisdictions (e.g., China).
Vendor Characteristics: Does the vendor understand the potential risks at issue with its data and what is its culture of compliance?	Given the variety of methods that may be used to obtain and transform data (some of which may not be realistic for Firms to verify independently), understanding the vendor and its compliance practices may be just as important as understanding the data itself when assessing Alternative Data risk. When evaluating the risks of receiving and using data from a particular vendor, Firms may consider vendor characteristics by asking questions such as: • **How long has vendor been in business?** Tenure may often result in more mature compliance programs. • **Has the vendor been subject to regulatory scrutiny or other litigation?** Litigation may highlight issues to investigate further. • **Where is the vendor headquartered?** Jurisdiction-specific requirements (e.g., GDPR) may result in more compliant vendors. • **Who are the vendor's officers and executives?** Strong vendor leadership, including with a proven track record in the financial services industry, may result in more compliant vendors. Alternatively, if vendor leadership has faced regulatory scrutiny or class action litigation, additional due diligence may be warranted. • **Does the vendor utilize reputable outside counsel?** Vendors' use of recognized law firms (e.g., to develop data compliance programs and advise on regulatory compliance), may result in more sophisticated vendors.
Market Adoption: How many financial services firms are using the data?	Firms may also ask a vendor how many financial services firms are using the dataset at issue to gain comfort that others have performed due diligence and approved the data/vendor. Even though Firms have varying risk tolerances, these variations may be normalized when taken in the aggregate. • **How many financial services firms must be using the data?** There is no agreed-upon number to represent "industry consensus"; for example, some Firms may view 5+ financial service firms using the data as satisfactory, while other Firms may set a threshold of 10+ firms.

Other Factors: Was there anything else about the data or the vendor that requires additional scrutiny by the Firm?	In addition to the factors described above, Firms may decide to consider other factors that might affect their view of the legal or reputational risk associated with a vendor or dataset. These factors may be informed by the judgment and experience of the Firm and may be informed by the Firm's risk tolerance. Examples of such factors include: • **Uncooperative/unresponsive vendor**: While diligence requests can be burdensome, a vendor's unwillingness to provide reasonable and necessary information can be a red flag. • **Maturity of vendor's compliance program**: Firms must often make subjective assessments of the maturity of the vendor, its agents, and its compliance program (if any). These assessments are informed by the totality of the communications between a Firm and a vendor. • **Inconsistent vendor responses**: Unexplained inconsistencies between diligence materials collected and statements made by the vendor can be a red flag. • **Media coverage**: There may be news coverage about a firm, a dataset, or even a category of dataset that could be viewed either positively or negatively.
Legal Review & Due Diligence	With respect to any dataset that exhibits potential Alternative Data characteristics based on the factors above, the Firm will review the materials provided by the vendor (and follow up with the vendor as needed for further information) in order to determine if the dataset should be classified as Alternative Data. • For any datasets that are classified as Alternative Data, the Firm will perform a due diligence analysis that is appropriately tailored to the dataset, vendor and risks at issue. • For any datasets that are NOT classified as Alternative Data, the Firm may memorialize this determination, negotiate the license agreement, and decide to forego or reduce the amount of due diligence analysis required. Once a dataset has been identified as exhibiting Alternative Data characteristics, and prior to using such information in trading, Firms must take reasonable steps to address and resolve potential compliance issues posed by the Alternative Data in question, consistent with and to the satisfaction of Firms' specific compliance requirements. The following due diligence processes may be used by Firms with respect to each Alternative Dataset: • **Due Diligence Questionnaires ("DDQ")**: The Firm will coordinate with the vendor to respond to, revise, and finalize, a due diligence questionnaire. Firms may develop their own DDQ templates or use a third party DDQ template such as the one developed by FISD. Firms may request that vendors review and update their DDQs periodically from time to time, which may necessitate further review and due diligence. • **Independent verification of vendors' DDQ responses**: Based on the circumstances of the data and vendor under review, the Firm may choose to undertake further due diligence measures including, but not limited to: i) requesting supplemental documentation from the vendor (e.g., data dictionary, upstream agreements, compliance policies); and ii) reviewing information discovered by the Firm (e.g., litigation history, news articles). • **Diligence documentation**: In addition to the completed DDQ, the Firm may document the steps that were taken to verify that the data and vendor are in compliance with relevant laws, rules and regulations, which may include a legal due diligence memo, record of diligence steps taken, including consulting with outside counsel, if applicable. The importance of such robust due diligence is underscored by market regulators' increasing scrutiny of the Alternative Data industry for several years, including the SEC's first enforcement action against an alternative data provider for securities fraud in 2021, and the SEC issuing a Risk Alert on alternative data in April 2022.