



BUSINESS CONTINUITY PLAN & INCIDENT RESPONSE NOTIFICATION DISCLOSURE

The Baker Group LP has developed and maintains a business continuity plan (BCP) to address possible disruptions to our normal course of business as a broker-dealer. This plan is reviewed and tested no less than annually, and updated as necessary. The BCP summarizes the actions that The Baker Group LP will take to ensure that its business is not materially disrupted in the event of a building-, city-, or region-wide disruptive event. The Firm has established and maintains redundant system capabilities at a secure off-site disaster recovery facility located in Oklahoma City, OK. Internal testing of the efficacy of these redundancies is conducted no less than annually by key Firm personnel. In the event a significant business disruption may occur, and depending on the nature of the disruption, it may be necessary to relocate key Firm personnel to the Firm's disaster recovery site facility.

The Firm maintains its hard copy and digital books and records at the Oklahoma City, OK office location. Digital records are backed-up no less than once daily by the copying of data located on the Firm's local network server to network server located at the Firm's disaster recovery site facility. Additionally, a back-up hard drive is created on the 15th of each month and is transported to a secure location for permanent storage.

Hard copy reports generated on behalf of our clients are stored on office premises for a period of 30 days. Reports are downloaded to our website and are accessible by customers with a valid password. As with the hard copy version, the online versions are available for the 30-day period following the date the version was first generated. The website server is maintained at an out-of-state location.

The approximate recovery time for business resumption, including relocation of key personnel or technology, is four (4) hours. This recovery objective may be negatively impacted by the availability of external resources and circumstances beyond the Firm's control.

In the event of a significant business disruption, customers may email their fixed income sales representative at their current email address by substituting @bakerbackup.com for @gobaker.com, or compliance personnel by emailing compliance@bakerbackup.com.

Cyber-intrusion Incident Notification

Forty-seven states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private entities to notify individuals of security breaches of information involving personally identifiable information.

Should the Firm experience a cyber-intrusion incident, the Firm will invoke its BCP to the extent that the nature of the incident requires it. If the nature of the incident includes the exposure of non-public information (NPI) belonging to an institutional customer of the Firm, or personally identifiable information (PII) belonging to a non-institutional customer of the Firm or to a customer of an institutional customer, the Firm will notify any customers affected as required by and in accordance with the laws that govern such notifications in the state in which the customer is incorporated or domiciled.

Contact our compliance department at compliance@gobaker.com with any questions regarding the Firm's business continuity plan or incident response notification protocols.