

LEWIS YOUNG ROBERTSON & BURNINGHAM

BUSINESS CONTINUITY PLAN

Lewis Young Robertson & Burningham is a registered broker dealer with the NASD with membership in the MSRB and SIPC. Its two main areas of business are:

- ☞ The provision of financial advisory services to municipalities, primarily located in the State of Utah. These services are related to the incurrence of debt on the part of the firm's municipal customers and run the full gamut of traditional financial advisory services. This would also incorporate special assessment district administration along with investment advisory services.
- ☞ What the firm refers to as non-bond related consulting services such as impact fee studies, economic feasibility, utility rate analyses, redevelopment agency feasibility analyses, annexation impact studies, among others.

The purpose of this document is to outline a business continuity plan ("BCP") by which the firm can insure the continuity of its business and its continued uninterrupted provision of services to its clients should a calamity affect the physical premises of its office. Currently, the firm has no branch offices. Other than a depository for funds, the firm has no relationship with other broker / dealers. The firm does not act as counterparty in any contractual relationship nor does it have such obligations.

It should be first noted that Lewis Young Robertson & Burningham does not handle customer funds, does not sell securities, does not underwrite securities, does not trade securities and has no clearing or other relationships with any broker dealer. The one exception is that the firm does have an account with a broker dealer for the deposit of the firm's operating cash. Therefore, the BCP as written below recognizes the firm's business and is tailored to allow for its core businesses to remain viable in the case of a business disruption at its office.

1. Data Back-up and Recovery

The firm is highly dependent upon its computer network system which includes three servers, one for email, one for data and programs and one for access. All employees of the firm are connected to the network and all electronic files, programs, data and email communications are accessed by each employee via the network. All employees have the capability of connecting to the network via remote access which is actively and routinely used by over half of the employees. Preserving the data stored on the network is of paramount importance to the BCP.

A. Hard Copy

Each individual is responsible for the maintenance of specific transaction files pertaining to engagements for which they have primary responsibility. When engagements are complete, a “closed deal file” is created and placed in the appropriate spot in the file room. If the engagement pertains to a financing, the bond counsel involved will provide a transcript of the transaction, a copy of which is maintained in the file room. It is now routine to also have a CD of the transcript. Every bond counsel retains a copy of the transcript. In addition, one is held by the municipality involved as well as by the trustee and/or paying agent.

Because of the “electronic trail” associated with each engagement, the loss of any hard copies of files would not create an inability of the firm to continue on with its business so long as the electronic files were intact. This is described below.

Most relevant documents to a transaction, even while in progress, are held at more than one location. For instance, a municipality will have its financial records on file and all parties authoring written communications will most likely maintain a copy. It would, however, be appropriate, when cost effective, for the firm to consider scanning certain important documents onto its network.

B. Electronic

Every night the servers automatically run a back-up tape of all the data stored on the networks servers. The next day, this back-up tape is removed from the office by one of the employees. The person primarily responsible for the oversight of the back-up tape is Stephanie Webb. When that person is not in the office then Lisa Johansen is designated. Each day the old back-up tape is returned and the new one is removed. In this fashion all data, being a maximum of one day old, will be stored in a separate physical place than the office.

On a monthly basis, a second copy of the back-up tape is removed from the office by a partner of the firm and recycled every month.

2. Mission Critical Systems

Since the firm does not trade or sell securities and does not handle customer funds in any manner, as defined in NASD Rule 3510(f)(1), the firm does not have any mission critical systems.

3. Financial and Operational Assessments

It is unclear if the definition of financial and operational assessment in NASD Rule 3510(f)(2) pertains to the operations of Lewis Young Robertson & Burningham.

Regardless, during the annual review of the BCP, the firm will determine what, if any, changes need to be made to accommodate its then current business.

The firm utilizes the services of two outside firms. Halliday & Company is the firm's outside accountant. It compiles a complete monthly financial summary of the firm's operations which is held in hard copy and electronically offsite at their offices. In addition, Halliday & Company files the firm's tax returns each year so has access to that information. The firm has retained Jones Simkins to perform its audit each year. As a result, certain financial information is available at their office.

4. Alternate Communications between Customers and the Firm

In the event of a disruption of business at its office location, each employee who has client contact responsibility will use their cell phone (all presently have them) to make contact with their customer municipalities. Each such employee also has a lap top computer and a separate internet account which will allow for electronic communications to be reestablished with the firm's customers.

5. Alternate Communications between the Firm and its Employees

With the use of the back-up tapes discussed above, a new server and network can be reconfigured with minimal loss of data. As with customers, each employee has a cell phone all employees have a list of cell phone numbers offsite to facilitate communications.

6. Alternate Physical Location of Employees

As noted above, many of the firm's employees regularly work from their home or other remote locations as a matter of course. All critical employees have been provided with lap top computers. Once a new network is reestablished, it will be possible for all employees to access the firm's network from their home or an alternate site.

7. Critical business constituent, bank and counter-party impact.

The major issues to contend with would be access to the firm's checking and investment accounts. Since no customer funds are involved the most prominent issue would be for the firm to be able to access its funds to pay for necessary continuing operational costs. The checkbook is now held on site. The firm maintains funds in two institutions, First National Bank and Smith Barney. Both have a number of branches so access to funds should not be an issue.

8. Regulatory Reporting

The only regulatory filings now required on the part of the firm are quarterly FOCUS reports and quarterly G-37 / G-38 reports. Both of these are completed electronically. It is important to have access to the firm's BD number, at a minimum, to be able to reach the NASD for the firm's password if the latter is not readily available. The person(s) responsible for filing the aforementioned reports will carry with them the necessary numbers and/or passwords.

Because filing is completed electronically, as required by the NASD and MSRB, it will be necessary to insure that the responsible person(s) have access to a lap top computer with internet access. As mentioned above, this is now the case expect for the person filing the G-37 / G-38 reports. If an interruption to business at the firm's office requires, access will be provided to the employee responsible.

9. Communication with Regulators

In the event of a disruption of business, the firm will immediately make contact with the Denver District office to inform them of the extent to which business has been disrupted, the likely impact upon the firm's ability to conduct business and the estimated time it will take to implement the actions called for in this BCP.

10. Miscellaneous

All employees of the firm will have been instructed to keep, in a safe place, outside of the firm's office, key passwords and related information to allow them to access data and other important information from a remote site.

The firm has designated Scott J. Robertson, a registered municipal principal, as the person responsible to implement the BCP and to conduct an annual review of the BCP. If changes are warranted, Mr. Robertson will make appropriate recommendations to the firm.

April 2006