Denial of Access to Technology

In the event that one technology system becomes inaccessible to staff this will be dealt with using normal IT service continuity management procedures.

In the event that the US Data Centre technology infrastructure or resilient communication links are not functioning (e.g. severe weather, fire, flood, un-remediated power-cut or bomb), key staff will continue to work in the main office using their main office workstation. All services will be delivered via a backup WAN link from Sacramento to the main office. Inbound and outbound telephony will continue to be available.

Denial of Access to Staff (Sudden)

In the event that main office staff suddenly becomes inaccessible to the main office and each other (e.g. severe weather, severe transport disruption), key staff will continue to work at home using remote access technology to remotely control their main office workstation desktop. All services will continue to be delivered to the office workstation in the normal way and from the normal point of origin. Inbound telephony will be remotely diverted to appropriate remote staff corporate cell phones.

Denial of Access to Staff (Pandemic)

Denial of Access to Office and Technology/ Denial of Access to Staff and Technology

This low probability risk (e.g. catastrophic act of God or terrorism; unrelated incidents simultaneously affecting the office, staff and/or data center) is mitigated by the fact that the US Data Centre is located outside of New York City and on a separate power grid.

In such event key staff will continue to work remotely at home using remote access technology to connect to virtual machines hosted at the Backup Data Centre (located in Sacramento). Inbound telephony will be remotely diverted to appropriate offsite staff cell phones An assumption is made that any incident which would deny access to both the main office and the US Data Centre – or main office staff and US Data Centre - would be catastrophic and that financial markets would close for a substantial period of time.

Denial of Access to Office and Staff (Sudden)

In the event that the main office becomes inaccessible to staff with the technology infrastructure not functioning (e.g. fire, flood, un-remediated power-cut or bomb) at the same time as staff suddenly become inaccessible to the main office and each other, key staff will continue to work at home using remote access technology to connect to virtual machines hosted at the Backup Data Centre (located in Sacramento). Inbound telephony will be remotely diverted to appropriate offsite staff corporate cell phones

Xtellus has also contracted with various entities to insure that sensitive information is made redundant at back-up facilities. However, due to the nature of such information we do not disclose the specific location of any back-up facilities, any proprietary information contained in our Business Continuity Plan or the parties with whom we have back-up arrangements.

Please call if you have any questions at 646-527-6400.

Thank you.

Stephen Zak, COO
Xtellus Capital Partners, Inc.

SEC RULE 17a-3(a)(18) - CUSTOMER INQUIRIES

Dear Client or Investor:

SEC Rule 17a-3(a)(18) requires our Firm to maintain a record indicating that each client or investor has been provided with a notice containing the address to which you may transmit any inquiries or complaints that you may have respecting our Firm.

Additionally, our Firm must ensure that you are provided with a notice indicating the telephone number and the address at our Firm to which such inquiries or complaints may be directed.

Xtellus Capital Partners, Inc. hereby provides the following address and telephone number to which any customer inquiries or complaints may be directed:

Xtellus Capital Partners, Inc.
Attn: Paul Swigart, CEO
535 Madison Avenue, 5th, Floor
New York, NY 10022
Tel (646) 527-6400

XTELLUS
CAPITAL PARTNERS

FINRA RULE 2266 - SIPC INFORMATION

As a member of the Securities Investor Protection Corporation (SIPC) funds are available to meet customer claims up to a maximum of $500,000 in cash and securities, with a $250,000 cash maximum. This protection is provided by the Securities and Investors Protection Act, which is administered by SIPC and is subject to certain conditions and limitations, details of which are available upon request. Information about SIPC, including the SIPC brochure, may be obtained by contacting SIPC: SIPC Web site address (www.sipc.org) SIPC telephone number (202-371-8300).

ANNUAL ORDER ROUTING DISCLOSURE

Reg NMS Rule 606 Annual Written Notice on Availability of Order Routing Information.

Quarterly Reports: Will identify the significant venues, as define in the rule, where orders were routed in listed equity securities and listed options, as well as order routing details. You may obtain the URL address to the public Web site or request a printed version by contacting Xtellus Capital Partners, Inc.

Investor Inquiry: You may request your specific order routing information in writing for the preceding six (6) months from the date of request. This will include the identity of the marketplace where the orders were routed for execution, whether the orders were directed or non-directed, and, if executed, the time of the execution. You may contact Xtellus Capital Partners, Inc. or additional details on the information that is available.

From time to time, Xtellus Capital Partners, Inc. may provide aggregated trade execution data to customers and prospective customers.