XTELLUS
CAPITAL PARTNERS

Anti-Money Laundering
Customer Identity Verification Notice

To help the government fight the funding of terrorism and money laundering activities, federal law requires broker-dealer firms to obtain, verify, and record information that identifies each person who opens an account.

What types of information will you need to provide?

For an entity, when an account is opened, we are required to collect information such as the following from the entity: documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

For an individual, when you open an account, we are required to collect information such as the following from you: Your name, date of birth, address, identification number: U.S. Citizen: taxpayer identification number (social security number or employer identification number) or Non-U.S. Citizen: taxpayer identification number, passport number, and country of issuance, alien identification card number, or government-issued identification showing nationality, residence, and a photograph of you. You may also need to show your driver's license or other identifying documents.

We may, under the following circumstances, rely on the performance by another financial institution (including an affiliate) of some or all of the elements of the our customer identification program with respect to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions.

Such reliance is reasonable under the circumstances, when the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements and is regulated by a Federal functional regulator and when the other financial institution has entered into a contract with us requiring it to certify annually to us that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the customer identification program.

Xtellus Capital Partners, Inc.

Notice of Privacy

This privacy notice complies with the Gramm-Leach-Bliley Act and federal regulations governing the privacy of financial information applicable to our clients.

Xtellus Capital Partners, Inc. Notice of Privacy

We are committed to providing our clients with quality service. While collecting information about you is essential to meet your needs, we recognize the importance of handling your personal information with care. Accordingly, we have established this Notice of Privacy and related policies.

Confidentiality and Security of Your Information

We maintain appropriate physical, electronic, and procedural safeguards to protect the security and confidentiality of your nonpublic personal information. We educate our employees about the terms of this Notice and the importance of customer privacy. We restrict access to nonpublic personal information about you to those employees and others who need to know that information to provide services to you, to maintain your accounts, or conduct our business.

Information We Collect About You

Collecting information from you is essential to our ability to offer quality services. As part of that process, we may collect nonpublic information about you from the following sources:

- Information we receive from you on applications and other forms;
- Information about your transactions with us;
- Based upon the services provided, information we receive from consumer reporting agencies, government agencies and from your agent banks and prime brokers where applicable; and
- Information that is used to facilitate emails from you.

Categories of Information We Disclose and to Whom

We do not disclose any information about our clients or former clients to anyone, except as permitted or required by law. We may disclose the types of information listed below to companies that help us conduct our business, that perform administrative or others services on our behalf, or other financial institutions with which we now or may have joint marketing agreements:

- Information we receive from you on applications and other forms, such as your name, address, Social Security number (if an individual), assets, income and beneficiaries;
- Information about your transactions with us, or others; and
- Information we receive from a consumer reporting agency, government agencies and from your agent banks and prime brokers where applicable, and from other sources, such as information concerning credit worthiness and history, and certain information requested pursuant to US Patriot Act anti-money laundering prevention rules and regulations.

XTELLUS CAPITAL PARTNERS, INC.

BUSINESS CONTINUITY PLAN

SUMMARY DISCLOSURE STATEMENT

Xtellus Capital Partners, Inc. (“Xtellus”), pursuant to Financial Industry Regulatory Authority, Inc. (“FINRA”) rules, has created a Business Continuity Plan to address and guide our response to and recovery from Significant Business Disruptions (“SBDs”). Copies of this Summary Disclosure Statement shall be given to all clients at the time they open their accounts with Xtellus.

Xtellus’ Business Continuity Plan is subject to modification and an updated summary will be promptly sent to our clients. Alternatively, clients may obtain updated summaries by requesting a written copy by mail or fax.

In all of the following scenarios, Xtellus plans to continue business and our planned recovery time, depending upon the time of occurrence, should not exceed 24 hours from the time of the declaration of the SBD. Staff, telephone calls, and e-mails will return to their original location upon full restoration of service.

Denial of Access to Office

In the event that the main office becomes inaccessible to staff with the technology infrastructure still functioning (e.g. emergency services cordon or public disorder), key staff will continue to work at home using remote access technology to remotely control their main office workstation desktop or virtual 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 desks at the workplace recovery facilities or to appropriate remote staff corporate cell phones.

Loss of Operations at Office

In the event that the main office technology infrastructure becomes inoperable (e.g. fire, flood, unremediated power-cut), key staff will continue to work at home using remote access technology to access basic applications. All services will continue to be delivered from the normal point of origin. Inbound telephony will be remotely diverted to appropriate desks at these workplace recovery facilities or to appropriate remote staff corporate cell phones.

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)

In the event that main office staff gradually become inaccessible to the main office and each other through pandemic spread, key staff with similar functions will split locations between normal office working and working at home using remote access technology to remotely control their main office workstation desktop. This will minimize the opportunity for cross-contamination within a single function. Pandemic responses will remain aligned with (and triggered by) guidance from the WHO and local health authorities. 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 offsite staff corporate cell phones. Office staff telephony will be unaffected.

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.