Privacy of Client Information

Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA") which repealed Section 20 of the Banking Act of 1933, commonly known as the Glass-Steagall Act, requires financial institutions, i.e. broker-dealers, to develop privacy policies with regard to consumer nonpublic information. In response thereto, the Securities and Exchange Commission ("SEC") promulgated Regulation S-P.

Information Collected and Shared

B&D Capital Partners, LLC's (BDCP) privacy policy statement is given to clients at the initial signing of the client engagement. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. Ongoing delivery would be required if there are instances of continued relationships past each individualized transaction. BDCP may collect information about clients from the following sources:

- Information received from client; and
- Information provided by a consumer reporting agency.

Below are the reasons for which BDCP may share a client's personal information:

- With specific third parties as requested by the client; and
- For everyday business purposes such as to respond to court orders and legal investigations.

If a client decides to terminate the relationship with BDCP, BDCP will adhere to the privacy policies and practices as described in this manual, as updated.

Please note that BDCP has no affiliate relationships and consequently has no policy about the sharing of information with affiliate businesses.

Storing Client Information

BDCP uses various methods to store and archive client files and other information. BDCP also restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. In addition to electronic protection, procedural safeguards, and personnel measures, BDCP has implemented reasonable physical security measures at its home office location.

In addition to BDCP's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time.

To mitigate a possible breach of the private information, BDCP uses encryption software on all computers and carefully evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

BDCP does not maintain or serve customers on an ongoing basis and thus the release of private information unintentionally is a low risk. As such, we do not maintain a third party as larger firms do to maintain

procedural and physical safeguards on the gathering and retention (pursuant to SEC Rules 17a-3 and 17a-4) of "non-public personal information" defined as "personally identifiable financial information."

Identity Theft Red Flags

The CFTC (U.S. Commodity Futures Trading Commission), SEC (U.S. Securities and Exchange Commission), and many state regulators, have published rules concerning identity theft encouraging or requiring firms to train personnel to recognize "red flags" regarding possible identity theft of advisory clients. While many of these provisions may also be covered in the firm's broader privacy and AML (anti-money laundering) policies, the list below is a brief non-exhaustive listing of the items and information that all BDCP personnel should monitor and safeguard to guard against any breach of a client's identity:

SAFEGUARDING IDENTIFYING INFORMATION

- Individual client's social security numbers
- Corporate or other entity client's tax identification numbers and other information
- Individual driver's license number or other personal identification card

POTENTIAL CAUSES OF IDENTITY INFORMATION BREACHES

- Loss of theft of computers and/or other equipment
- Hacking of computer networks
- Inadvertent exposure of client information to unauthorized individuals (non-locked files, files left on desk, cleaning services, shredding services, etc.)
- Physical break-ins / theft
-

BDCP personnel are instructed to notify the firm if they detect or have reason to believe that any of the above shown red flag activities may have occurred or if any of the red flag information listed may have been stolen or leaked by any firm personnel. The CCO is then tasked with investigating the report and taking appropriate actions. The non-exhaustive list of possible follow-up actions includes notification of the parties involved, notification of appropriate regulatory officials if required, taking remedial actions to assist in the recovery of the stolen information, and possible sanctions of firm personnel if deemed necessary.

Staff Training

On an annual basis, BDCP will conduct a firm-wide training session to ensure that staff members are properly trained and equipped to implement the above policies regarding client privacy. New staff members will receive training, led by the CCO, within one (1) month of their initial hire date.

Client Records

Client engagement records will be retained by BDCP for at least six years after the year in which the record was produced, or as otherwise required by law. With respect to disposal of non-public personal information, BDCP will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.

BDCP takes the privacy and confidentiality of all its clients and personnel very seriously. It will continue

to make, and document, any changes needed to promote the security of client information. Additional safeguards are described in the Cybersecurity & Information Security Policy section of this manual.