



**SLOAN
SECURITIES
CORP.**

PRIVACY POLICY

The following information contains Sloan Securities Corp.'s ("Sloan") privacy policy designed to protect the confidentiality of current or former customers ("you") of Sloan. Your relationship with Sloan was established when you opened a brokerage account. We receive your nonpublic personal information for the sole purpose of servicing your account. This information is presented to you in conformity with Regulation S-P, 17 CFR 248.1-248.3, under Title V of the Gramm-Leach-Bliley Act, codified as 15 U.S.C. 6801-6831. The nonpublic personal information which identifies you or your account is hereafter referred to as "personal information". Maintaining personal information securely and confidentially is a Sloan priority. The following information will explain our privacy policy in more detail.

YOUR NONPUBLIC PERSONAL INFORMATION

SLOAN DOES NOT SELL YOUR NONPUBLIC PERSONAL INFORMATION. WE WILL ONLY DISCLOSE YOUR NONPUBLIC PERSONAL INFORMATION, WHICH INCLUDES ANY PERSONALLY IDENTIFIABLE INFORMATION ABOUT YOU, AS INDICATED IN THIS POLICY, IF WE HAVE OBTAINED YOUR CONSENT OR WE ARE REQUIRED BY LAW TO DISCLOSE SUCH INFORMATION.

NONPUBLIC PERSONAL INFORMATION COLLECTED

In order to provide you with the highest quality of service, Sloan collects the following types of nonpublic personal information:

Information from you:

Information you provide on an application for an account, a margin loan, debit card or any other financial product or service, whether in writing, in person, by telephone, electronically or by any other means, such as your name, address, social security number, assets, income, and debt; and Information we obtain for the purpose of tax reporting to you and to the various agencies to which we report as required by law, including disclosures on various Internal Revenue Service (IRS) forms that we collect for tax reporting purposes.

Information about your transactions with us:

Information that relates to account balances, payment history, trading activity and any other such transactions for which Sloan provides services; Information we collect as part of authentication for purposes of servicing your account in a secure and confidential fashion; and Information we may collect through an Internet "cookie" (an information collecting device from a web server).

Information about your transactions with nonaffiliated third parties:

Information provided to nonaffiliated third parties as required by law, including information shared in connection with a subpoena or other legal document compelling our compliance; and Information related to servicing your account for purposes of services.

Information from a consumer-reporting agency:

Information from a consumer reporting agency regarding your creditworthiness or credit history or other information as it pertains to lending; Information about the fact that you are a customer of Sloan and we have provided you a financial product or service; and

Information from other outside sources regarding their employment of, credit to, or other relationship with you, or verifying representations made by you, such as your employment history, loan or credit card balances.

NONPUBLIC PERSONAL INFORMATION DISCLOSED

Nonpublic personal information is disclosed in connection with servicing your account for the purposes of providing services which includes, among other things, settlement, billing, processing, clearing, transferring, reconciling, collection and tax reporting.

AFFILIATES AND NONAFFILIATED THIRD PARTIES TO WHOM WE DISCLOSE

Sloan does not disclose any nonpublic personal information about you except as permitted by law.

FORMER CUSTOMERS

Sloan will only disclose nonpublic personal information about former customers as required by law or upon your request.

PRIORITIZING SECURITY OF INFORMATION

Sloan is committed to maintaining appropriate measures to insure that your information is secure and confidential. Sloan's information and security procedures include, but are not limited to, the following features: Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means; Physical access restrictions at locations containing customer information, such as buildings, computer facilities, and record storage facilities to restrict access to unauthorized individuals; Stringent pre-employment screening, including fingerprinting, background checks and verification of previous employment; Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems; A disaster recovery plan to protect against loss of or damage to customer information due to potential environmental hazards, such as fire and water damage or technological failures.