XANTOS LABS

PRIVACY POLICY/REGULATION S-P

Effective April 2019

Overview

Xantos Labs LLC has developed Client Privacy Policy/Regulation S-P. The Company views protecting its customers' private information as a top priority and, pursuant to the requirements of the Gramm-Leach-Bliley Act (the "GLBA"), the Company has instituted the following policies and procedures to ensure that customer information is kept private and secure.

This policy serves as formal documentation of the Company's ongoing commitment to the privacy of its customers. All employees will be expected to read, understand and abide by this policy and to follow all related procedures to uphold the standards of privacy and security set forth by the Company. This Policy, and the related procedures contained herein, is designed to comply with applicable privacy laws, including the GLBA, and to protect nonpublic personal information of the Company's customers.

In the event of new privacy-related laws or regulations affecting the information practices of the Company, this Privacy Policy will be revised as necessary and any changes will be disseminated and explained to all personnel.

Scope of Policy

This Privacy Policy covers the practices of the Company and applies to all non-public personally identifiable information of our current and former customers.

Overview of the Guidelines for Protecting Customer Information

In Regulation S-P, the SEC published guidelines, pursuant to section 501(b) of the GLBA, that address the steps a financial institution should take in order to protect customer information. The overall security standards that must be upheld are:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

Employee Responsibility

- Each employee has a duty to protect the nonpublic personal information of customers collected by the Company.
- No employee is authorized to disclose or use the nonpublic information of customers on behalf of the Company.
- Each employee has a duty to ensure that nonpublic personal information of the Company's customers is shared only with employees and others in a way that is consistent with the Company's Privacy Notice and the procedures contained in this Policy.
- Each employee has a duty to ensure that access to nonpublic personal information of the Company's customers is limited as provided in the Privacy Notice and this Policy.

- No employee is authorized to sell, on behalf of the Company or otherwise, nonpublic information of the Company's customers.
- Unauthorized dissemination of proprietary information and client personal and sensitive data is prohibited and a violation of Regulation SP. This includes sending client nonpublic information to personal emails. Unauthorized downloading of confidential client information to a thumb or zip drive is prohibited. Should the Company suspect an employee has downloaded information to a thumb or zip drive, our IT will have the capability to determine if such information was downloaded on an external mechanism.
- Employees with questions concerning the collection and sharing of, or access to, nonpublic personal information of the Company's customers must look to the Company's CCO for guidance.
- Violations of these policies and procedures will be addressed in a manner consistent with other Company disciplinary guidelines.

Information Practices

The Company collects nonpublic personal information about customers from various sources. These sources and examples of types of information collected include:

- Product and service applications or other forms, such as customer surveys, agreements, etc. – typically name, address, age, social security number or taxpayer ID number, assets and income;
- Transactions - account balance, types of transactions and investments;
- Other third-party sources.

Disclosure of Information to Nonaffiliated Third Parties – "Do Not Share" Policy

The Company has a "do not share" Privacy Policy. It does not disclose any nonpublic personal information about customers or former customers to nonaffiliated third parties. Under no circumstances does the Company share credit-related information, such as income, total wealth and other credit header information with these nonaffiliated third parties.

Types of Permitted Disclosures – The Exceptions

Regulation S-P contains several exceptions which permit Xantos to disclose customer information (the "Exceptions"). For example, Xantos is permitted under certain circumstances to provide information to non-affiliated third parties to perform services on the Company's behalf. In addition, there are several "ordinary course" exceptions which allow Xantos to disclose information that is necessary to effect, administer or enforce a transaction that a customer has requested or authorized. A more detailed description of these Exceptions is set forth below.

1. **Service Providers.** The Company may from time to time have relationships with nonaffiliated third parties that require it to share customer information in order for the third party to carry out services for the Company. These nonaffiliated third parties would typically represent situations where Xantos or its employees offer products or services jointly with another financial institution, thereby requiring the Company to disclose customer information to that third party. Every nonaffiliated third party that falls under this exception is required to enter into an agreement that will include the confidentiality provisions required by Regulation S-P, which ensure that each such

nonaffiliated third party uses and re-discloses customer nonpublic personal information only for the purpose(s) for which it was originally disclosed.

2. **Processing and Servicing Transactions.** The Company may also share information when it is necessary to effect, administer or enforce a transaction for our customers or pursuant to written customer requests. In this context, “Necessary to effect, administer, or enforce a transaction” means that the disclosure is required, or is a usual, appropriate or acceptable method:
    - To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the consumer's account in the ordinary course of providing the financial service or financial product;
    - To administer or service benefits or claims relating to the transaction or the product or service of which it is a part;
    - To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the consumer or the consumer's agent or broker; or
    - To accrue or recognize incentives or bonuses associated with the transaction that are provided by the Company or any other party.
3. **Sharing as Permitted or Required by Law.** The Company may disclose information to nonaffiliated third parties as required or allowed by law. This may include, for example, disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, an audit or examination, or the sale of an account to another financial institution. The Company has taken the appropriate steps to ensure that it is sharing customer data only within the Exceptions noted above. The Company has achieved this by understanding how the Company shares data with its customers, their agents, service providers, parties related to transactions in the ordinary course or joint marketers.

Provision of Opt Out

As discussed above, Xantos currently operates under a “do not share” policy and therefore does not need to provide the right for its customers to opt out of sharing with nonaffiliated third parties. If our information sharing practices change in the future, Xantos will implement opt-out policies and procedures and make appropriate disclosures to our customers.

Safeguarding of Client Records and Information

The Company has implemented internal controls and procedures designed to maintain accurate records concerning customers’ personal information. The Company’s customers have the right to contact the Company if they believe that Company records contain inaccurate, incomplete or stale information about them. The Company will respond in a timely manner to requests to correct information. To protect this information, Xantos maintains appropriate security measures for its computer and information systems, including the use of passwords and firewalls.

Additionally, the Company will use shredding machines, locks and other appropriate physical security measures to safeguard client information stored in paper format. For example, employees are expected to secure client information in locked cabinets when the office is closed.

Security Standards
Xantos maintains physical, electronic and procedural safeguards to protect the integrity and confidentiality of customer information. Internally, Xantos limits access to customers' nonpublic personal information to those employees who need to know such information in order to provide products and services to customers. All employees are trained to understand and comply with these information principles.

Privacy Notice
Xantos has developed a Privacy Notice, as required under Regulation S-P, to be delivered to customers initially. The notice discloses the Company's information collection and sharing practices and other required information and has been formatted and drafted to be clear and conspicuous. The notice will be revised as necessary any time information practices change. Xantos would notify clients of any change to this Privacy Notice.

Privacy Notice Delivery

Initial Privacy Notice - As regulations require, all new customers receive an initial Privacy Notice at the time when the customer relationship is established, for example on execution of the agreement for services.

Revised Privacy Notice Regulation S-P requires that the Company amend its Privacy Policy and distribute a revised disclosure to customers if there is a change in the Company's collection, sharing or security practices.

Regulation S-ID – Identity Theft Red Flag Rules Applicable to Investment Advisors
Our Firm's policy is to protect our customers and their accounts from identity theft and to comply with the Red Flags Rule. These rules apply to any account belonging to an individual consumer (a Covered Account). Xantos currently manages no Covered Accounts. When the Firms does, they will continue to comply with these rules by developing and implementing a written Identify Theft Prevention Program (ITPP), which will be appropriate to our size and complexity, as well as the nature and scope of our activities. Xantos expects that the ITPP will address 1) identifying relevant identity theft Red Flags for our Firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.