Portfolio ThinkTank Privacy Policy

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 confidential and proprietary personal information of the company's advisory customer's clientele.

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.

A. Scope of policy

This privacy policy covers the practices of the company and applies to all confidential and proprietary personally identifiable information of our current and former advisory customer's clientele.

B. Overview of the guidelines for protecting customer information.

In regulation s-p, the securities and exchange commission (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.

C. Employee responsibility

- Each employee has a duty to protect the confidential and proprietary personal information of advisory customer's clientele collected by the company.
- No employee is authorized to disclose or use the confidential and proprietary information of advisory customer's clientele on behalf of the company.
- Each employee has a duty to ensure that confidential and proprietary personal information of the company's advisory customer's clientele 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 confidential and proprietary personal information of the company's advisory customer's clientele is limited as provided in the privacy notice and this policy.
- No employee is authorized to sell, on behalf of the company or otherwise, confidential and proprietary information of the company's advisory customer's clientele.
- Employees with questions concerning the collection and sharing of, or access to, confidential and proprietary personal information of the company's advisory customers clientele 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.

.

Dd. Types of permitted disclosures – the exceptions

Regulation s-p contains several exceptions which permit Portfolio ThinkTank to disclose customer information (the "exceptions"). For example, Portfolio ThinkTank 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 Portfolio ThinkTank 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 Portfolio ThinkTank or its employees offer products or services jointly with another financial institution, thereby requiring the company to disclose customer information to that third party.

PORTFOLIO
THINKTANK

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.

D. Opt out.

As discussed above, Portfolio ThinkTank 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, we will implement opt-out policies and procedures and make appropriate disclosures to our customers.

E. 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, Portfolio ThinkTank 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 measure 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.

F. Security standards

Portfolio ThinkTank maintains physical, electronic and procedural safeguards to protect the integrity and confidentiality of advisory customer's clientele information. Internally, Portfolio ThinkTank limits access to advisory customers' clientele's 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.

G. Privacy notice

Portfolio ThinkTank has developed a privacy notice, as required under regulation s-p, to be delivered to customers initially and every July from that point forward. 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. A copy of Portfolio ThinkTank 's privacy notice is included as appendix d.

A. Infrastructure

Our database and web servers are mounted on amazon web services which has strong security policies on different layers from administering the servers to running our applications.

On our application

www.gsphere.net
www.gravityinvestments.com
www.PortfolioThinktank.com

Our entire application runs on top of an authentication/authorization mechanism that verifies user permissions on each requested resource. Additionally, all sensitive data is encrypted to prevent common web attacks.

Our security protocols are reviewed not less than annually to ensure that our security standards are current for the privacy needs of all clients and investors.

On the client-side (browser)

All communication runs on top of http over SSL protocol to guarantee the information is encrypted on both ends, the browser and the server.

See more from amazon:

https://aws.amazon.com/security/

H. Privacy notice delivery

1. **Initial privacy notice -** as regulations require, 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.

2. **Annual privacy notice -** the GLBA regulations require that disclosure of the privacy policy be made on an annual basis.

I. 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.