Privacy

Self Audit Checklist

I. While your strategy for achieving compliance will depend on the complexity of your firm and the progress it has already made in complying with the requirements of the privacy rule, the following progression of action steps should be a part of any effort to develop an effective and comprehensive privacy compliance strategy:

☐ **Assess Current Information Collection and Sharing Practices.** Existing practices with respect to nonpublic personal information must be reviewed in order to:

- ☐ (1) Ensure that these practices are properly disclosed in the firm's privacy notices;
- ☐ (2) Determine the extent to which disclosures to third parties fall within the rule's exceptions;
- ☐ (3) Evaluate if any information sharing would trigger opt out rights for consumers; and
- ☐ (4) Determine whether any practices are prohibited (*e.g.,* impermissible sharing of account numbers with third parties). This process should also include agreements with nonaffiliated third-party service providers who market your firm's products or services. The privacy rule requires your firm to enter into a contract limiting the third party's use of disclosed consumer information.

☐ **Develop Privacy Policies and Notices.** The privacy rule requires that all firms, even those that do not share nonpublic personal information, provide privacy notices to consumers. By creating a list of information collection and sharing practices that must be disclosed to consumers, you can categorize practices per the rule requirements and decide how to structure notices. Your initial and annual privacy notices will most likely be identical. If an opt out notice is required, it may be combined with the initial and annual notices.

☐ **Deliver Notices.** You must determine the mechanism for delivering notices to customers, consumers, and joint account holders. It is important to identify all groups of existing customers, consumers, and former customers who must get the initial privacy notice and the opt out notification. Methods of delivery include hand delivery, mail, and electronic delivery where the consumer is conducting business with the firm electronically and agrees to this method of delivery**. Firms that intend to share consumer information subject to opt out rights must deliver notices well before next July 1.**

☐ **Develop Opt Out Procedures.** All firms sharing nonpublic personal information with nonaffiliated third parties outside of the exceptions will need to develop procedures for consumers to exercise an opt out and for processing and complying with opt out directions. Opt out procedures should include:

- ☐ (1) Tracking the initial opt out period which is generally the first 30 days after delivery of the notice;
- ☐ (2) Recording opt outs received from consumers;
- ☐ (3) Maintaining the opt method(s), such as a toll-free phone number, electronic mail, or an opt out form; and
- ☐ (4) Complying with opt out directions received after the initial opt out period elapses.

☐ **Develop Policies and Procedures to Safeguard Customer Information.** These policies and procedures, which must be disclosed in your privacy notices, should address administrative, technical, and physical safeguards for customer information.

II. The Checklist provided below has been designed to assist you in achieving and maintaining compliance with the privacy rule as your business changes.

Determine type of clients you have:

- ☐ Institutional or Business (not covered by the privacy rule)
- ☐ Consumer
- ☐ Customer
- ☐ Former Customer

List of third parties with which you share information:

☐ 1._____ ☐ Affiliate ☐ Non-affiliate

☐ 2._____ ☐ Affiliate ☐ Non-affiliate

☐ 3._____ ☐ Affiliate ☐ Non-affiliate

Tip: Non-affiliated third parties include organizations such as non-profit groups, retailers, direct marketers, insurance agents, CPAs, broker-dealers, investment advisers, etc.

Check the information that is shared with the above:

- ☐ Name
- ☐ Address
- ☐ Phone number
- ☐ Email address
- ☐ Account Number
- ☐ Social Security Number
- ☐ Credit scoring information
- ☐ Financial information obtained from a credit report
- ☐ Transaction information
- ☐ Account balance information
- ☐ Any financial information obtained through the application process (assets, liabilities, credit information, etc)

☐ Annual Privacy Notices will be sent every year on _____(Date).

☐ Initial Privacy Notices will be sent on _____(Date - must be prior to July 1, 2001).

Privacy policies and procedures regarding:

- ☐ Collecting nonpublic personal information.
- ☐ Using, sharing and disclosing nonpublic personal information.
- ☐ Process to monitor implementation of consumer's opt out decision. (Examples: decision may only effect a particular product or service, joint customers and only one opts out.)
- ☐ Contracts with third-party service providers or joint marketers.
- ☐ Safeguards to insure the security and confidentiality of customer records.
- ☐ Safeguards to protect against anticipated threats or hazards to the security or integrity of customer records.
- ☐ Safeguards to protect against unauthorized access to or use of customer records that may result in substantial harm or inconvenience to clients. (Examples: employee resignation, unlisted telephone numbers, maintenance of opt out notices, restricting internal use/access to a need-to-know basis.)
- ☐ Policy regarding the timing and method of delivering of initial and annual notices.
- ☐ Inclusion of sample notices in manual on an ongoing basis.
- ☐ Policy for verifying delivery of initial notice. (Example: include notice with application and have client initial receipt of such on the application.)

Web site review:

- ☐ Privacy statement on website
- ☐ Provide statement as to how firm collects and /or deals with Internet "cookies"

Employee training:

- ☐ Do all employees understand privacy policies and firm's procedures for complying with the rule?
- ☐ Employees who have direct consumer contact should be able to answer simple privacy inquiries.
- ☐ All employees should be aware of prohibition against sharing account number information for marketing purposes.

Develop controls to monitor ongoing compliance:

- ☐ Delivery of initial and annual notices to customers
- ☐ Delivery of initial notice to consumers who are not customers, if applicable
- ☐ Compliance with opt out directions, if applicable
- ☐ Ongoing accuracy of privacy notices, including prior approval for:
  - ☐ New marketing agreements
  - ☐ New or renewed vendor contracts
  - ☐ Disclosure of account numbers
  - ☐ Affiliate-referral programs
  - ☐ Reuse of consumer information received from another financial institution
  - ☐ New products or services
  - ☐ Mergers/acquisitions
- ☐ Scheduled audits/compliance reviews

