Privacy Notice Policy

Revision Date: 2/26/2024

1. Overview

Section 502-509 of title V of the Gramm-Leach-Bliley Act (GLBA), and its implementing Regulation P, (also known as the Privacy Rule) requires financial institutions to provide notice to customers about their privacy policies and practices; describe the conditions under which they may disclose nonpublic personal information about consumers to nonaffiliated third parties; and provide a method for consumers to prevent companies from disclosing that information to most nonaffiliated third parties by opting-out of that disclosure. Furthermore, the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA) contain provisions to ensure protection of the financial information of consumers

2. Definitions

The following definitions apply to this Policy:

- **Consumer** – means an individual who obtains or has obtained from a financial institution a financial product or service that is to be used primarily for personal, family, or household purposes and includes such an individual's legal representative. A consumer includes an individual who provides nonpublic personal information in order to obtain a determination about whether he or she qualifies for a loan. A consumer also includes an individual who applies for a loan, regardless of whether credit is extended to that person.
- **Customer**– means a consumer who has a "customer relationship" with a financial institution. A "customer relationship" is a continuing relationship between a consumer and a financial institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.
- **Nonpublic Personal Information** – means any information that is not publicly available and that a consumer provides to a financial institution to obtain a financial product or service from the institution; results from a transaction between the consumer and the institution involving a financial product or service; or a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

3. Policy Statement

SteadyNest requires all employees, affiliates, and service providers to comply with all consumer protection regulations regarding the privacy and disclosure of consumer information. SteadyNest also complies with all disclosure requirements regarding its privacy policies and practices by providing customers with a privacy notice that clearly describes SteadyNest's practice of collecting, protecting, and sharing customer's nonpublic personal information (NPI) with affiliates and third parties at the time that a customer relationship is established. Wherever local privacy regulations are more stringent than the requirements set forth in this Policy, the more stringent requirement will be followed.

SteadyNest will send a copy of the privacy notice to all new customers in the timeframes specified in the Privacy Rule. SteadyNest will also provide a privacy notice annually during the continuation of the customer relationship, if applicable.

4. Privacy Notice Requirements

SteadyNest complies with the following privacy notice requirements under the GLBA and, when applicable, the FCRA. Further, the GLBA provides that SteadyNest will obtain a "safe harbor" and will satisfy the disclosure requirements for notices if it chooses to use the model form provided under the GLBA.

A. Initial Privacy Notices

SteadyNest is required to provide an initial privacy notice to customers when a customer establishes a relationship with SteadyNest by providing any personally identifiable financial information in an effort to obtain a mortgage loan.

SteadyNest is also required to provide a consumer a privacy notice before sharing NPI with nonaffiliated third parties outside of the exceptions described below. If SteadyNest doesn't share information with nonaffiliated third parties, or if it only shares within the exceptions, SteadyNest does not have to provide a privacy notice to consumers.

If SteadyNest is required to provide a privacy notice to consumers, it may choose to give a "short-form notice" instead of a full privacy notice. The short-form notice must:

- explain that SteadyNest's full privacy notice is available on request;
- describe a reasonable way that consumers may obtain the full privacy notice; and
- include an opt-out notice.

B. Annual Privacy Notices

SteadyNest also sends annual privacy notices to their customers during the continuation of the customer relationship, if applicable. The annual notice must accurately describe SteadyNest's privacy policies and practices in effect at the time the notice is sent.

Annually means at least once in any period of 12 consecutive months during which that relationship exists. SteadyNest does not send privacy notices after the relationship with the customer has ended.

C. Information Included in Privacy Notices

The privacy notice includes:

- The categories of NPI that SteadyNest collects;
- The categories of NPI that SteadyNest discloses;
- The categories of affiliates and nonaffiliated third parties to whom SteadyNest discloses NPI;
- The categories of NPI about former customers that SteadyNest discloses and the categories of affiliates and nonaffiliated third parties to whom SteadyNest discloses NPI about former customers;
- If SteadyNest discloses NPI to a nonaffiliated third party, a separate statement of the categories of information it discloses and the categories of third parties with whom SteadyNest has contracted;
- An explanation of the consumer's right under Regulation P §1016.10(a) to opt-out of the disclosure of NPI to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time;
- Any disclosures made under section the Fair Credit Reporting Act (that is, notices regarding the ability to opt-out of disclosures of information among affiliates); and

- SteadyNest policies and practices with respect to protecting the confidentiality and security of NPI.

D. Exceptions to Privacy Notice Requirement

Exceptions for processing transactions at consumer's request – Exceptions to the initial privacy notice, opt-out and for service providers and joint marketing do not apply if SteadyNest discloses NPI as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes, or in connection with:

- Servicing or processing a financial product or service that a consumer requests or authorizes;
- Maintaining or servicing the consumer's account with SteadyNest, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or
- A proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer.

5. Opt-Out Notice

Opt-out means a direction by the consumer that SteadyNest may not disclose NPI about that consumer to a nonaffiliated third party, other than as permitted by law. The opt-out notice is a clear and conspicuous notice to all customers that accurately explains the right to opt-out under that section. The notice states:

- that SteadyNest discloses or reserves the right to disclose NPI about a consumer to a nonaffiliated third party;
- that the consumer has the right to opt-out of that disclosure; and
- a reasonable means by which the consumer may exercise the opt-out right.

A. Exceptions to Opt-Out Notice

The requirements for initial notice and for service providers and joint marketing do not apply when SteadyNest discloses NPI:

- With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;
- To protect the confidentiality or security of SteadyNest records pertaining to the consumer, service, product, or transaction;
- To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- For required institutional risk control or for resolving consumer disputes or inquiries;
- To persons holding a legal or beneficial interest relating to the consumer or acting in a fiduciary or representative capacity on behalf of the consumer;
- To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating SteadyNest, persons that are assessing SteadyNest compliance with industry standards, and SteadyNest attorneys, accountants, and auditors;
- To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including the Bureau, a Federal functional regulator, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, with respect to any person domiciled in that insurance authority's state that is engaged in providing insurance, and the

Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

- To a consumer reporting agency in accordance with the Fair Credit Reporting Act;
- From a consumer report reported by a consumer reporting agency;
- In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of NPI concerns solely consumers of such business or unit;
- To comply with Federal, State, or local laws, rules and other applicable legal requirements;
- To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by Federal, state, or local authorities; or
- To respond to judicial process or government regulatory authorities having jurisdiction over SteadyNest for examination, compliance, or other purposes as authorized by law.

6. Revised Notices

The Privacy Rule is designed to enable consumers to make opt-out decisions based on an accurate description of a financial institution's privacy policies and practices. Before disclosing NPI about a consumer to a nonaffiliated third party other than as described in SteadyNest's most recent privacy notice, SteadyNest must provide the consumer a revised initial notice, a new opt-out notice, and reasonable opportunity to opt out.

A revised notice is not required in the instance where SteadyNest makes a change to disclose NPI to a new nonaffiliated third party that was adequately described in its prior notice.

7. Delivery Requirements

SteadyNest provides the required privacy and opt-out notices simultaneously. SteadyNest provides privacy notices and opt-out notices so that each consumer can reasonably be expected to receive actual notice in writing. The notice can be hand-delivered, mailed, or, if the consumer consents, delivered electronically.

8. Prohibition on Disclosure of Account Notices

The Privacy Rule prohibits financial institutions from sharing account numbers or similar access numbers or codes for marketing purposes. This prohibition applies even when a consumer or customer has not opted out of the disclosure of NPI concerning his or her account.

Under no circumstances will SteadyNest disclose, other than to consumer reporting agencies, access codes or account numbers for use in marketing.

9. Limitations on Redisclosure or Reuse of NPI

When a financial institution receives NPI from a nonaffiliated financial institution, its disclosure and use of the information is limited as follows:

- For NPI received under any of the privacy and opt-out notice exceptions outlined above, the financial institution is limited to:
    - Disclosing the information to the affiliates of the financial institution from which it received the information;

  - Disclosing the information to its own affiliates, who may, in turn, disclose and use the information only to the extent that the financial institution can do so; and
  - Disclosing and using the information pursuant to any of the privacy and opt-out notice exceptions outlined above (for example, an institution receiving information for account processing could disclose the information to its auditors).
- For NPI received other than under any of the privacy and opt-out notice exceptions outlined above, the recipient's use of the information is unlimited, but its disclosure of the information is limited to:
  - Disclosing the information to the affiliates of the financial institution from which it received the information;
  - Disclosing the information to its own affiliates, who may, in turn disclose the information only to the extent that the financial institution can do so; and
  - Disclosing the information to any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which it received the information.

10. Fair Credit Reporting Act and Privacy

The Fair Credit Reporting Act (FCRA), among other things, allows financial institutions to share information with others about their own transactions or experiences with a consumer. However, when a financial institution shares information about third-parties' transactions with a consumer, such as sharing a list of its customers and information such as their credit scores with another financial institution to jointly market or sponsor other financial products or services, it could cause the financial institution to be considered a consumer reporting agency that is subject to strict guidelines under FCRA. Furthermore, civil or criminal penalties could apply if a financial institution fails to comply with any requirements of the FCRA.

Financial institutions can avoid additional requirements and penalties under FCRA by not providing others with information from credit reports or third-party transactions. Additionally, FCRA contains an exception that allows financial institutions to share information contained in consumer reports and other information, such as information on an application for credit, as long as that information is shared with an affiliate and before the information can be used for marketing and solicitation, the financial institution:

- clearly and conspicuously discloses to the consumer that the information may be shared with an affiliate; and
- gives the consumer the opportunity, before the information is shared, to opt-out of having their information shared.

The GLBA notice is sufficient to meet FCRA notice requirements for sharing information with affiliates. Furthermore, the FCRA notice and opt-out requirements do not apply to a financial institution if it uses eligibility information that it receives from an affiliate to make a solicitation for marketing purposes to a consumer with whom the financial institution has a preexisting business relationship.

11. The Right to Financial Privacy Act

The Right to Financial Privacy Act (RFPA) protects a customer's right to privacy with respect to information being disclosed to the federal government regarding the financial records maintained about the customer by financial institutions. The RFPA is intended to balance the federal government's need for information when conducting a criminal investigation with the customer's right to privacy. It establishes specific procedures that federal government authorities must follow in order to obtain information from a financial institution about a customer's financial records. Generally, these requirements include obtaining subpoenas, notifying the customer of the request, and providing the customer with an opportunity to object.

Under the RFPA, the government must reasonably describe the records it wants and may use one of five methods to obtain those records:

- **Customer Authorization**

  Under this method the customer must give a signed and dated authorization to both the government and the institution. Further, the authorization must state the customer's rights under the RFPA. In this document, the customer must:
  - Authorize the disclosures for no more than 3 months.
  - State that the authorization can be revoked at any time before records are disclosed.
  - Identify the records to be disclosed
  - Specify the purpose for which, and the government authority to which, records may be disclosed.

- **Administrative Subpoena or Summons**

  A government authority may obtain financial records using an administrative subpoena or summons if there is reason to believe the records are relevant to a legitimate law enforcement inquiry. A copy of the subpoena or summons must have been served to the customer, or mailed to the customer's last known address, on or before the date on which it was served to the financial institution and it should include a notice regarding the nature of the law enforcement inquiry and notify the customer of his or her right, and procedures, to contest the inquiry.

- **Search Warrants**

  Search warrants must be obtained according to the federal rules of criminal procedure. The customer must receive a copy of the search warrant no later than ninety days after it is issued and receive a notice of his or her rights under the RFPA.

- **Judicial Subpoena**

  A government authority can obtain financial records under a judicial subpoena only if there is a reason to believe the records are relevant to a legitimate law enforcement inquiry. When a judicial subpoena is issued, the subpoena must have been served to the customer, or mailed to the customer's last known address, and it must state the nature of the law enforcement inquiry and notify the customer of his or her right, and procedures, to contest the inquiry.

- **Formal written request**

  A government agency may request financial records using a formal written request only if all of the following conditions are met:
  - The government agency doesn't appear to have legal authority to issue a summons or subpoena;
  - The request is authorized by regulation issued by the head of the agency; or

- There is reason to believe the records are relevant to a legitimate law enforcement inquiry.

When a formal written request is used, it must have been served to the customer, or mailed to the customer's last known address, and it must state the nature of the law enforcement inquiry and notify the customer of his or her right, and procedures, to contest the inquiry.

The RFPA also contains exceptions for depository institutions under 12 US Code Section 3413, allowing these institutions to, among other things, disclose:

- financial records that are not identified with or identified as coming from a particular customer;
- customer financial records to its supervisory agencies;
- financial records or information required by federal statute; and
- financial information in accordance with procedures authorized by the IRS.