

**[Community Association name]**  
**Identity Theft Prevention Program**  
**Policy and Procedures**  
**Policy**

[Community association name (“Association”)] strictly complies with all federal and state laws and reporting requirements regarding identity theft, including the federal Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This policy outlines the Association’s Identity Theft Prevention Program (“Program”), which is mandated by the Red Flags Rule and governs how Association will (1) identify, (2) detect and (3) respond to “red flags.” A “red flag” is defined as a pattern, practice, or specific account or record activity that indicates possible identity theft.

The Program must be approved by [Association *Board of Directors or appropriate committee of the Board, or someone in senior management if there is no Board*] as of November 1, 2009, and the Program must be reviewed and updated at least once a year in order to ensure that the Program keeps current with identity theft risks. In doing so, [Association *Board of Directors or appropriate committee of the Board, or someone in senior management if there is no Board*] will consider the Association’s experiences with identity theft situations and similar experiences for other entities in the community association industry, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in Association’s business arrangements with other entities.

It is the Association’s policy that [*specify title of a senior employee*] is assigned the responsibility of overseeing, developing, implementing, and administering the Program. Association is committed to ensuring that this individual, designated as Association’s privacy official, be provided with sufficient resources and authority to fulfill these duties.

Association requires that its business associates be contractually bound to protect sensitive client information to the same degree as set forth in this policy. Business associates of the Association who violate their agreement will be dealt with first by an attempt to address the problem, and if that fails, by termination of the agreement and discontinuation of services by the business associate.

Association’s workforce must be trained on the policies and procedures governing compliance with the Red Flags Rule, and new workforce members are required to receive training on these matters within a reasonable amount of time after they have been hired. Should any policy or procedure related to the Red Flags Rule materially change, the Association shall provide further training within a reasonable amount of time after the policy or procedure materially changes. All training sessions are to be documented, indicating participants, date, and subject matter.

**Procedures**

- I. Identify red flags.** While providing community services to homeowners, the Association may encounter inconsistent or suspicious documents, information, or activity that suggests the possibility of identity theft. The following are identified as potential red flags:
1. Notice from a homeowner, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently
  2. A dispute of a bill or assessment by a homeowner who claims to be the victim of any type of identity theft

3. Suspicious documents, such as paperwork that appears altered or forged, and information on the identification that is inconsistent with other information, like a signature card or recent check
4. Suspicious personal identifying information, such as inconsistencies with what is already known and inconsistencies in the information the homeowner has already provided.
5. Suspicious account activity, such as an account that is used in a way inconsistent with established patterns, an account that has been inactive for a long time that is suddenly used again, and information that the homeowner is not receiving their account statements in the mail
6. [Insert other relevant items here.]

**II. Detect Red Flags.** Employees of the Association will be alert for discrepancies in documents and homeowner information that suggest risk of identity theft or fraud. The Association staff will verify homeowner identity and address before services are provided and billed. Specifically, the procedures for detecting red flags are as follows:

1. When somebody notifies the Association that an account has been opened or used fraudulently, employees are required to report such notifications to their immediate supervisor or the designated privacy official. If reported to a supervisor, that supervisor should relay the information to the privacy official
2. When verifying the identity of a homeowner who is opening a new account, Association staff are required to obtain a name, address, and identification number and, for in-person verification, to check a current government-issued identification card, such as a driver's license or passport
3. Regarding existing accounts, the Association staff is expected to verify the identification of homeowners if they request information, and verify the validity of change-of-address requests and changes in banking information given for billing purposes
4. In general, Association staff should be alert for the possibility of identity theft in the following situations:
  - The photo identification submitted by the homeowner does not resemble the homeowner
  - Identifying information submitted by the homeowner appears to be altered or forged.
  - Information on one form of identification the homeowner has submitted is inconsistent with information on another form of identification or with information already in the records kept by Association
  - An address or telephone number is discovered to be incorrect, non-existent, or fictitious
  - The homeowner fails to provide identifying information or documents
  - The homeowner's signature does not match a signature in the homeowner's records
5. [If programs are already being used to mitigate identity theft, such tools should also be listed here.]

**III. Respond to Red Flags.** If any employee of Association detects fraudulent activity or if a homeowner claims to be a victim of identity theft, Association will respond to and investigate the situation.

If potentially fraudulent activity (a red flag) is detected by an employee of the Association:

1. The employee should gather all documentation and report the incident to his or her immediate supervisor or the designated privacy official. If reported to a supervisor, that supervisor should relay the information to the privacy official
2. The privacy official will determine whether the activity is fraudulent or authentic
3. If the activity is determined to be fraudulent, then Association should take immediate action, which may include the following:
  - Canceling the transaction;
  - Closing an existing account;
  - Reopening an account with a new account number;
  - Not opening a new account;
  - Not trying to collect on an account or not selling an account to a debt collector;
  - Notifying appropriate law enforcement;
  - Notifying the affected homeowner; and
  - Changing any passwords or other security devices that permit access to accounts.

If a homeowner claims to be a victim of identity theft, the following procedures should be followed:

1. The homeowner should be encouraged to file a police report for identity theft if the homeowner has not done so already.
2. The homeowner should be encouraged to complete the ID Theft Affidavit developed by the Federal Trade Commission, along with supporting documentation.
3. Association will compare the homeowner's documentation with personal information in the homeowner's records.
4. If, following investigation, it appears that the homeowner has been a victim of identity theft, the Association will promptly consider what further remedial act/notifications may be needed under the circumstances.
5. If, following investigation, it does not appear that the homeowner has been a victim of identity theft, the Association will take whatever action it deems appropriate.