

Red Flag Rules Policy & Procedure

Company Name:
Street Address:
City, State and ZIP:

Responsible Individual:
Phone:
E-mail:

- I. **Application:** This policy and procedure is a written identity theft prevention program developed by the Company as required by the Fair and Accurate Credit Transactions (FACTA) Act of 2003. The Company has determined based on Federal Trade Commission (FTC) regulations that the Company is by definition a “creditor” with “covered accounts” and thus is subject to the “Red Flag Rules.”
- II. **Purpose:** The purpose of this policy and procedure is to develop a customized program for the Company that will identify, detect, and respond to business practices or specific activities referred to as “Red Flags” that could result in identity theft. The programs must include procedures to protect against potential identity theft and provide a remedial procedure should identity theft occur.
- III. **Responsibility:** The Red Flag Rules requires that an individual within the Company be designated with the responsibility to oversee the program. For purposes of the program, the responsible individual (designated above) will have the following responsibilities; (1) oversee the implementation of the program, (2) monitor the program’s effectiveness, (2) be diligent in identifying any “Red Flags” not initially identified for the program or created by a procedural change within the company and revise the written program accordingly, (3) take the appropriate actions prescribed in this program should an identity theft or potential identity theft occur, (4) review the program when office procedures are revised or when a potential breach of identity security is identified, (5) periodically but not less than semi-annually review the program, and (6) insure that each employee has read and understands the program.
- IV. **Staff Training:** All existing employees and any future new hires are required to review this document and adhere to policies and procedure contained herein.
- V. **Identified Red Flags:** “Red Flag” Rules generally focus on identity theft associated with a creditor’s covered accounts which has very limited applicability to this company, which only extends credit to clients for accounting, tax preparation and related services that are only of value to the individual to which they are provided. The company does not sell a tangible product which a thief can convert to their own use nor does the company advance cash to covered account holders that a potential thief can access.

The greater threat to identity theft for a company providing accounting, tax preparation and related services come from the internal procedures employed by the company and the transferring of data between the company, the client, and contractors providing services to the company.

The company has identified the following Red Flags and provided associated prevention procedures (policy solutions) as follows:

- 1) **Mailing documents to an incorrect address** – There is the possibility of mailing documents to a client at a prior address or to the address of another client, thus exposing a client’s identity information to a third party.

***Policy Solution** – Each time a service is provided for a client, the client’s current address must be verified and the appropriate client files updated.*

- 2) **Sending documents to clients via e-mail** – E-mail is not a secure medium; there is always the chance of someone hacking into it and gaining access to sensitive documents that include a client’s identity information.

- Policy Solution** – Whenever sending documents that include a client’s or potential client’s identity information, convert them to password protected PDF or ZIP files that only the recipient can open with the correct password. Another option would be to use a password-protected internet lockbox.
- 3) **New clients attempting to file fraudulently** - There is the remote possibility of someone in possession of a stolen identity attempting to have a fraudulent tax return prepared for various reasons.
- Policy Solution** – Ask new clients for some sort of ID, keeping in mind that identity thieves could also be in possession of forged documents. If there is any suspicion raised by the documents presented that do not match the client’s age, general description, suspicious addresses, etc., then additional verification is required that a thief would probably not be in possession of such as birth certificates, utility bills, etc.
- 4) **Unsecured client files** – Clients and others come and go frequently in an accounting and tax preparation business office. Client files left unattended on office work spaces are susceptible to being stolen or having data copied.
- Policy Solution** – Do not leave files unattended in the presence of anyone. Do not allow unescorted office visitors in office areas where client files are stored.
- 5) **E-file rejection** – When e-filing tax returns, the IRS will reject those where the name and SSN do not match the Social Security Master file. There is a chance that the client may be using someone else’s ID in an attempt to secure an illicit refund.
- Policy Solution** – If the client is new and the rejection cannot be traced to a reasonable cause, ask for additional verification including items that would not be included in a stolen wallet or purse.
- 6) **Requests for client data** – It is not uncommon to receive requests for certain client information from attorneys, financial planners, brokers, lenders and even other tax preparation firms preparing another entity return of the client. Providing information to unsubstantiated requests could lead to disclosure of information that will result in identity theft.
- Policy Solution** – IRC Code Section 7216 and its regulations preclude tax preparers from disclosing tax return information to third parties without a client’s written consent. This Company shall not provide any third party any information related to the client without the client’s written permission. The Company shall make every effort to avoid the third party disclosure and the need for client consents by providing the information directly to the client who can then forward the information to the third party.
- 7) **Technical assistance** – Occasionally, the Company may seek assistance from other professionals or peers outside of the firm. Frequently, there is a need for the other professional to review and analyze certain documents as part of the provided assistance. Not knowing whether the other professional is compliant with the Red Flag Rules can cause the Company to be non-compliant.
- Policy Solution** – As a company policy, all client documents provided to other professionals outside of the Company shall have all client identity made illegible by some appropriate means whether by cutting out with scissors, blacking with a magic marker, or other suitable means. The exception to this rule is where IRC Code Section 7216 and its regulations permit disclosures without client consent and where the professional from whom the assistance is requested is compliant with the Red Flag Rules.
- VI. **Responding to Red Flags** – If red flags are detected, the service being provided shall be immediately suspended until the red flag issue is resolved. Where it is determined that there was or is a possibility that client identity information has been compromised, the affected clients shall be immediately notified. Where criminal activity is evident, the appropriate authorities should be notified.
- VII. **Contractors** – The Red Flag regulations make the Company responsible for insuring that every contractor from which the Company receives services and shares client identity is Red Flag compliant. As a matter of policy, the Company will make inquiries to insure all of its contractors are also compliant. For the tax and accounting business, this would include but is not limited to an e-file provider, certain software providers where the client data is hosted by the software provider, and credit card processing companies.

This policy is adopted by the Company effective _____, 2009.

By: _____ Title: _____