

**NICK J. STORHAUG, CPA
PO BOX 669
LISBON, ND 58054**

(701) 683-5303

RED FLAG COMPLIANCE RULES

An assessment of Nick J Storhaug, CPA

Date _____.

Reasons we are low risk for identity theft:

- 1) We are familiar with the majority of our clients; It is unlikely an identity thief could impersonate someone we know.
- 2) New clients are always interviewed and their documents examined.
- 3) We have been in business for over 26] years and no one has complained that their identity was used by someone else after our business services were concluded.
- 4) There are no reports in the news or talk among people in our area about any identity theft in our line of work.

Identifying Red Flags

- 1) Anytime you receive unusual information requests by phone or mail such as requests for Social Security Numbers, birthdates, bank information, addresses, or copies of tax returns and financial statements.
- 2) A person posing to be someone else; using fake identification.
- 3) A person asking for a copy of another's tax return unless a married spouse or parent of a minor child.
- 4) Someone not having proof of bank information for direct deposit of refunds.
- 5) Someone with documents that look altered, forged, or torn up and reassembled.

Detecting Red Flags

- 1) We will not release or transmit Social Security Numbers or Federal Identification numbers. We will answer requests, if possible, by calling the questioner back using their phone number in our files.
- 2) Persons suspected of posing as someone else will have to show a badge, second identification or business card.
- 3) No completed tax return will be given out unless it is to a married spouse or parent of a minor child unless the taxpayer has provided written consent. A copy of the consent form will be kept in the file.

- 4) A voided check or deposit slip with the clients name and address will be proof of bank account information.
- 5) We will ask clients for more information if documents look altered or reassembled.

Response to Red Flags

- 1) Nick Storhaug, CPA, owner of the company, and program administrator, will deal with any notice from a client, victim of identity theft, a law enforcement agency, or someone else that has had an account that had been opened fraudulently.
- 2) Employees will inform Nick Storhaug as soon as possible after a request for unusual information has been made or if there is a suspicion of someone posing as someone else.
- 3) When clients are interviewed, all other files will be put away from that client's view.
- 4) We will shred all papers containing names and Social Security Numbers and/or Federal Identification Numbers.
- 5) Only employees who have signed a privacy agreement will have access to company computers.
- 6) Computer service personnel will also sign confidentiality agreements.
- 7) All files will be locked up at night.

Administering the Red Flag Procedures

- 1) A staff meeting will be held to inform all employees of the Red Flag Procedures.
- 2) There will be a staff meeting every year to review and update any Red Flag Procedures.
- 3) There will be an index card by every telephone to remind employees about the data that cannot be released by telephone.

Red Flag Program Approval

Our program has been approved by _____, Program Administer