

**IMPORTANT: IN ORDER TO PREPARE RETURNS IN A TIMELY MANNER,
ALL INFORMATION FOR PERSONAL AND BUSINESS TAX RETURNS MUST BE SUBMITTED TO US BY AUGUST 10TH .**

PAGE 1

JULY 2006

**T. Dennis Connally Consultant, P.C.
Certified Public Accountant**

Financial

The Network Group and T. Dennis Connally Financial Consultants, Inc.

THE TOTAL SOLUTION

The total solution for your business' challenges and opportunities

General Business Consultant

Loan Request Packages

SBA

Analysis

Conventional

Financial Review with your:

Pricing

Bank

Analysis

Financial Institution

Control

Bonding Company

Statement &

Insurance Company

Analysis

Financial Management

Budget

Cost Analysis

Product

Market

Expense

Cash Flow

Financial Statement

New Business Startups

Business Plans, Projections, & Proformas

Management & Collection of A/R, Notes, & other open accounts

Life Insurance Policy Conversion to Cash

Business Brokerage

**Business Sales or liquidations
Acquisitions & Mergers
Real Estate Sales & Management**

Resources

Accounting, Financial & Bookkeeping Services
Advertising & Marketing
Total Computer
Services

Please call Larry Grady at 770-920-2890 ext 10 or email
networkgroup@tdconnally.com

“We Mind Your Business”

**Network Business Consultants Inc. * Network Realty
Group, Inc.**

IDENTITY THEFT : OUTSMARTING THE CROOKS

How can someone steal your identity? Identity theft occurs when someone uses your personal information such as your name, Social Security number or other identifying information, without your permission, to commit fraud or other crimes.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years, and their hard earned money, cleaning up the mess thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing or cars, or even get arrested for crimes they didn't commit.

Generally, identity thieves use their victim's personal data to steal financial accounts and run up charges on their existing credit cards. However, the damage does not stop there. Identity thieves can also cause havoc with their victim's tax records.

How can you minimize becoming a victim?

- * Don't carry your SSN.
- * Don't give a business your SSN just because they ask-only when necessary.
- * Protect your financial information.
- * Check your credit report every 12 months.
- * Secure personal information in your home.
- * Don't give personal information over the phone, through the mail or on the internet unless you have initiated the contact or you are sure you know who you are dealing with.
- * Protect your personal computers by using firewalls, anti-spam/virus software, update security patches, and change passwords for internet accounts.

What if you are a victim of identity theft?

- * Report incidents of identity theft to the FTC at www.consumer.gov/idtheft or the FTC Identity Theft hotline at **877.438.4338** or **TTY 866.653.4261**.
- * File a report with the local police.
- * Contact the fraud departments of the three major credit bureaus:
 - Equifax-www.equifax.com
 - Experian-www.experian.com
 - TransUnion-www.transunion.com
- * Close any accounts that have been tampered with or opened fraudulently.

How could identity theft impact your tax records?

- * Individuals may use your SSN to get a job. That person's employer would report the W-2 wages earned using your SSN to IRS. This may give the appearance that you did not report all of your income on your return.
- * When you subsequently file your tax return, the IRS will believe you already filed and received a refund, and the return you actually submitted is a second copy or duplicate.
- * Be alert to possible identity theft if you receive an IRS notice or letter that states that:
 - *More than one tax return for you was filed, or
 - *IRS records indicate you received wages from an employer unknown to you.

What should you do if your tax records are affected by Identity Theft?

If you receive a notice from IRS, respond immediately. If you believe someone may have used your SSN fraudulently, please notify IRS immediately by responding to the name and number printed on the notice or letter.

What if you receive an e-mail claiming to be from the IRS?

- * The IRS does not initiate contact with taxpayers via e-mail.
- * Confirm the contact you have received is from the IRS by calling 800.829.1040.
- * Forward the bogus e-mail claiming to be from the IRS to phishing@irs.gov.
- * Do not open attachments or click on the links found within the bogus e-mail.

(This information was re-printed from the IRS Identity Theft Program brochure.)

The IRS publishes a DVD entitled Identity Theft-Outsmarting the Crooks. Obtain a copy from www.irs.gov (keyword *identity theft*).

Top Ten Tips to Help Prevent Fraud (in order of effectiveness)

1. Send Bank and Credit Card Statements to a Separate Address. Do not send your bank statements to your business address. Have your bank statement sent to your home, PO Box, or lockbox address. Review each check both front and back for payee, signature, and endorsement. Examine each statement carefully. Review each and every line item of both payments and charges.

2. Do Not Let Anyone Misrepresent Themselves as You. Do not let them or employees use

your password, sign your name, or use your credit card, ever. Reimburse their expense. Don't reveal sensitive passwords.

3. Reconcile Bank Accounts and Review Statements. Review every statement. Make sure all bank accounts and credit cards are reconciled. Notice stale checks or deposits that have not cleared the bank. Check for missing deposits.

4. Assign Administrative Rights Effectively. Use the Administrative rights in QuickBooks to protect your data. The first person to set up QuickBooks is by default assigned as Administrator. This role has unique permissions. So the administrator should be designated to either an outside party, i.e., a CPA, a QuickBooks Certified Consultant, or the savvy owner. Make sure that every user is set up separately and that passwords are used. Lock down permissions to change or delete transactions. **Especially important:** Use passwords for closing dates.

5. Use the Audit Trail in QuickBooks. If you don't have the latest version of QuickBooks, make sure you turn on the **Audit Trail**. Go to **Preferences > Accounting** and click on the box **Audit Trail**. **Caution:** the **Audit Trail** won't tell you if a vendor name has been changed or merged. It is wise to maintain a strict paper trail. Supporting documents need to be readily accessible in your files and then archived according to the type of document.

6. Use the Voided/Deleted Transaction Report. After you have turned on the Audit Trail, and made its review part of your routine, periodically review the **Voided/Deleted Transaction Report** to see which entries have been modified.

7. Establish Accounting Controls. The principle of countervailing power is the fundamental reason to use checks and balances in accounting. Split the responsibilities between staff members or outside accounting professionals. **Warning Sign:** If only one person writes the checks and reconciles the account, there is no double check. Separate the duties. Perhaps a Certified QuickBooks ProAdvisor® or CPA can provide these services.

8. Adhere to a Numerical Sequence. Use a numerical sequence for all transactions. Invoices, bills, and checks which are numbered fall in a logical and chronological order. The reason: to identify missing documents. Look at the bank statement for large gaps. Secure paper checks. If you keep voided paper checks, remember to tear off the signature area to keep it from being misused. If your bank sends paper checks, sort them numerically.

9. Review Receivables and Payables. Look for adjustments to **receivables** or **payables**. Such adjustments could indicate subverted payments or vendor checks.

10. Back up Your Data. Repeat after me – Back up, back up, back up. Think redundant backups as a contingency plan for disasters of all sorts. Make scheduled copies. Rotate the media (tape drive or portable storage). If you use CDs, better buy the read-only variety. Store your backups at another location. Such diligence can come in especially handy if there is a disaster.

Let us know if you have any questions. You can contact us at 770-920-2890 or tdconally@tdconnally.com.

December 31-Marital status on this date determines 2005 filing status.

We now have a 1-800 number! 1-866-724-5840