



Volume 8, Issue #3, October 2008

Visit
www.sunburstsoftwaresolutions.com

QuickBooks® for Contractors Newsletter

Protecting Yourself, Your Business, and Your Employees from Identity Theft

Identity theft occurs when a thief uses your personal information without your permission to commit a crime or fraud. They may find and use your credit card number on a bill you have thrown out or a stray receipt. They may use a device to capture your credit card number when you use it. And they may even fill out a change of address card and divert your statements.

Hundreds of thousands of people are affected by identity theft in the U.S. each year. Some victims have spent a lot of time and money repairing their credit rating and financial status. Other victims are unable to purchase cars, houses, or other items when they need them because of their "new" and unwelcome credit rating.

Below are some tips that you can take to protect yourself, your business, and your employees:

- **Protect Your Signature.** NEVER publish your real signature on your web site, in an email signature file, or anywhere else publicly. If you are in the habit of throwing out papers with your signature on it, purchase a shredder and shred them instead.
- **Protect Your Financial Identity.** Keep a shredder by every trash can where you throw out papers. Get into the habit of taking a good look at every piece of paper you throw out and shred each one that has your Social Security number, credit card number, driver's license number, or any other personal identifying number or information. This will reduce the risk of "dumpster diving" - which is a common practice whereby thieves go through your trash to find personal information.

You might be surprised at which papers have identifying information on them. You might need to shred mail that you don't even want to open - for example, credit card applications. Please be careful to inspect all papers just to make a systematic rule to shred everything.

- **Protect Your Financial Records.** Be careful who has access to your financial records, even in your own house. If you have lots of house guests, teenagers with numerous friends, or neighbors over all the time, you have a slight risk of exposure.

Keep your papers all in one place, and if possible, lock them up for safekeeping and limited access to people you trust. Don't forget about the papers you leave out on top of your desk or in a mail stack.

- **Protect Your Computer.** Do you have financial information on your computer? Password-protect both your computer and your financial files, and keep your password in a private, safe place.

- **Be Savvy on the Web.** Use good judgment when entering credit cards on web sites of businesses you don't know or when presenting your card to a business that looks questionable. This will reduce the risk of "skimming", where thieves posing as merchants steal your card number as they enter it on their device.

When making internet purchases, look for "hacker-safe" and "secure" shopping carts as these sites are more secure than others.

- **Be Wary of Email.** Never send your credit card number and security code in an email to someone. Never reply to an email that requests your personal information. If you think the email is real, go to your bank branch in person to check it out. This will reduce the risk of phishing, where the thief poses as a bank to get your information.
- **Be Cautious on the Phone.** If someone calls you, claiming to be from your Credit Card Company, bank, etc. and later asks for your personal information, be wary. It could be a setup, and it's very easy to fall for. The caller will get you engaged in solving a big problem with your account and you could let your guard down. Don't! If there's a question in your mind about whether it's real or not, ask if you can call them back, making sure you get their full name and a phone number, then, call the business using the phone number on the back of the credit card or in the phone book and ask to speak with that person.
- **Be Discreet.** Watch how you hold your credit card in a public place such as a line at the supermarket (cover the numbers). Don't say your credit card number in public and don't repeat it on a cell phone. This is a low risk but cell phone conversations are easily intercepted.
- **Stay Vigilant with Statements.** Make sure you receive your statements on a timely basis. If a statement is a few weeks late, follow up with the institution to find out why. Better yet, convert to online statements. This will avoid the risk of a thief changing your address and diverting the statements.
- **Keep Track of Your Reports.** Monitor your accounts: bank accounts, credit cards, and credit reports regularly.
- **Protect Your Employees.** Keep employment records under lock and key. Limit access to this data to only those employees who absolutely have to access it.

If you have to file Certified Payroll Reports, public documents which require you to provide employee names, addresses, and social security numbers, contact your local Department of Labor, Prevailing Wage Division and talk to them about your concerns in providing so much personally identifying information; if need be write a letter to the Labor Commissioner.

Important Note regarding the submission of Certified Payroll Reports – According to an article published in the Associated Builders & Contractors newsletter, the U.S. Department of Labor wage & Hour Division published a proposed rule on October 20, 2008 that would revise regulations relating to the Davis-Bacon and the Copeland Anti-Kickback Acts.

This proposed rule would eliminate the reporting of the home address and social security numbers of each employee on weekly certified payroll reports.

If you currently use our Certified Payroll Solution program, you already have the ability to "choose" how you wish to display employee social security numbers, see this article in our CPS

Technical Support Area - <http://www.sunburstsoftwaresolutions.com/view-document-details/changing-how-social-security-numbers-are-displayed-on-your-final-reports.htm>

More information on this proposed ruling is supposed to be available after November 19, 2008 and we will be monitoring this closely and making any necessary programming modifications.

For more information regarding this article from ABS, visit their website at http://www.abc.org/Newsroom2/News_Letters/2008_Archives/Issue_42/DOL_Proposed_Rule_Hopes_to_Protect_Worker_Privacy.aspx

- **Spread the Word.** Educate everyone in your household about these ideas so that they are not only fully implemented but teach them the importance of protecting their personal information.

If you discover fraudulent activity on your accounts, there are four things to do **immediately** (time is of the essence):

- Place a fraud alert on your accounts.
- Close your affected accounts.
- File a police report.
- File a complaint with the Federal Trade Commission (FTC).

The FTC has more information on their web site to help protect you from becoming a victim of identity theft: <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>



© 2000-2008 Sunburst Software Solutions, Inc. All rights reserved. This work is licensed under the Creative Commons Attribution-No Derivative Works 3.0 United States License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nd/3.0/us/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA. No part of newsletter may be reproduced in any form or by any means without prior agreement and written consent from Sunburst Software Solutions, Inc. QuickBooks® for Contractors Newsletter is a Free Service of Sunburst Software Solutions, Inc. QuickBooks® is a registered trademark of Intuit Inc. in the United States and other countries.