



Our mission is to provide information and strategies to business owners and managers for improvement in the effectiveness of its business management so that key objectives can be realized.

CFO Plus, LLC

Ted Hofmann - Principal/Senior Consultant

John Morre - Principal/Senior Consultant

Linda Panichelli - Principal/Senior Tax Consultant

1450 Grant Avenue, Suite 102

Novato, CA 94945-3142

Home Office: 415-898-7879

Toll Free 866-CFO-PLUS or 866-236-7587

Email: thofmann@cfoplus.net

jmorre@cfoplus.net

lpanichelli@cfoplus.net

Web: www.cfoplus.net

Identity Theft – Not What You Expect

Not too long ago, I traded in my carefree, apartment-living lifestyle for a mortgage in the burbs. Just as the United States Post Office recommends, my husband and I filled out our change of address cards and promptly put them in the mail two weeks before our move. After all, we had almost 30 days between residences to ensure all the mail flowed in the right direction. With all the free credit card offers we receive on almost a daily basis, we wanted to be sure all our mail safely reached our new home.

So, after doing everything by the book, imagine our surprise when our account was drained by thousands of dollars. We didn't realize it until we received our first bank statement – no signs of forced entry were about to alert us otherwise. Shortly thereafter, we learned that the bank's automated system, which we were told updates our new address for our checks, sent 400 checks to our old address. Apparently, the new occupants were having a field day with our checks.

That was more than a year and a half ago and they are still writing on the account. The irony of this story is we meticulously shred documents, we cancel credit cards on a schedule, we've even written about identity theft. How could this happen to us?

As they say, it's the little things that count. Simple items like double checking with the check printing company to ensure they have the correct address. And other things like not including personal information, such as driver's license numbers or social security numbers, on checks. Since then, the culprits have obtained fake IDs in both our names – luckily we didn't have our real numbers imprinted on the checks! The police officer assigned to our case told us that, most likely, once these individuals blow through our checks, they will start counterfeiting check stock with our information. Great.

Meanwhile, we continue to send affidavits of fraud to every check security company that notifies us of yet another one of these gems. The attorneys for these companies tell us we may be doing this for years.

Don't be a victim of identity theft – this is a billion dollar industry for criminals and it robs you of much more than productivity and performance on the job. Follow these 10 guidelines to keep an eye on what belongs to you.

1. **Guard your name and identification like they are gold.** Everyone from estranged spouses to roommates can use your good credit and identity by having just a few pieces of relevant information, such as a driver's license number, social security number or credit card accounts. They use tactics such as stealing wallets, digging through your trash and stealing your mail to obtain access to your information. These shrewd criminals commonly change your address to a post office box so they can intercept mail.
2. **Know where your information is and manage it.** Identity thieves can gain access to your vital credit information legally at the local courthouse if you are recently divorced and your filings contained credit card or social security numbers or other personal information. Take care to keep your information out of easy-access areas.
3. **Guard company data.** Many credit card offenders steal identities by securing a position within a company where he or she has access to employee databases. One recent case proved that identify theft was as simple as saving a company's employee roster, including social security numbers, to a disk and walking away. Put security systems in place to guard employee identities in your company. Fine-tuned internal controls can greatly reduce the chance of this happening.
4. **Put up your guard.** Use your work phone number or cell phone number on your checks instead of your home phone. If you have a post office box, use that instead of your home address, if you do not have a post office box, use your work address, if permitted. Never imprint your social security or driver's license number on your checks – you can add it if it is necessary, but know that in many retail situations, it is your right to deny this information.

Identity Theft – Not What You Expect (cont.)

5. **Plan for the worst.** Place the contents of your wallet on a photocopy machine; include both sides of each license, credit card, etc. This provides a record of what is in your wallet in the case of theft or loss. You will have all account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place.
6. **Leave home without it.** Unless you are going for your first day of employment or need to get a duplicate birth certificate, the chances of actually needing your social security card are slim to none. Better to leave this at home in a safe place until you really need it. This is one card you don't want to fall in the wrong hands.
7. **Fax anyone?** The health industry is making it easier to steal a social security number. Often, the primary card holder's social security number is the member number. While it doesn't make sense to forgo carrying your card, you can fax your new doctor ahead of time and carry a photocopy of your card with the number blacked out – just in case of emergency. The real card can stay at home with your social security card.
8. **Check in often.** The best strategy is a proactive one. Many options are available to check your credit report often to ensure there isn't any fraudulent activity on your account. One gentleman found that thieves opened more than 40 accounts before he found out about it.
9. **Just say no.** If you have great credit, chances are you get a LOT of those preapproved credit card offers in the mail. To stop these from filling your mailbox, simply contact the company and ask that they not contact you through the mail. Many companies contact current clients through email or phone calls. You always have a choice, so feel free to say, "no!"
10. **It happened...now what?** File a police report immediately in the jurisdiction where it was stolen, this proves to credit providers you were diligent, and is a first step toward an investigation (if there ever is one). Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. The numbers are: Equifax: 1-800-525-6285 Experian (formerly TRW): 1-888-397-3742 Trans Union: 1-800-680-7289 Social Security Administration (fraud line): 1-800-269-0271.

While we hope you never have to endure the agony of having your identity stolen. This is a growing crime against our currency-shy country. To learn more about how to protect your good name, visit www.consumer.gov/idtheft. This site offers forms and step-by-step instructions on how to handle identity theft.