

Precautions help when it comes to identity theft

By Scott A. Merritt

At least 110 million consumers were affected by the hack involving Target and Neiman Marcus retailers. Whether or not millions more will have their identities manipulated and finances ruined within the coming months due to more breaches of security at other stores is anyone's guess.

By necessity, I became an expert on identity theft. My information was stolen in 2006, and in repairing the damage, I learned some not-so-obvious ways we can all protect against identity theft in the first place.

My problems began quickly. While disputing financial charges and dealing with resulting business problems, in 2007 I was stopped for a traffic violation and arrested on a false outstanding felony warrant. I immediately knew why.

I had to enlist my U.S. congressman and convince the state police, NCIC, FBI and Secret Service that I didn't commit the felonies. For a few years, I had to prove that the prints did not match the false record in question. After legal action, however, I was able to have this corrected.

Unfortunately, the millions affected by the recent hacks may be dealing with similar repercussions in the years ahead.

Before you become a victim of identity theft, here are seven ways to guard against it.

- Understand how and where it happens. Identity theft is like being robbed when you are away from home; most thefts occur in places where you do business every day. Either a place of business is robbed, a bad employee acts improperly or a hacker

breaches the office through the computer.

- Secure your wallet's information. Photocopy everything in your wallet: photos, credit cards (front and back), membership cards – everything. Put the copies in the order the cards are arranged in your wallet, staple the pictures and place them in a strong box or safe.

- Make sure your information is consistent. For all of your identity and financial documents, make absolutely sure, to the smallest detail, that all of your personal information is accurate and consistent. Discrepancies such as using your middle initial on some documents, and not others, or having different addresses, can wreck havoc in proving your identity, and can compromise your credit score.

- Secure your digital habits and data. Change your passwords at least twice a year on a non-scheduled basis – don't be predictable. Have a strong firewall if you shop online, and only access sites that are protected by a strong firewall and high industry standards. Access accounts of a financial nature only from your personal computer.

- Protect your banking information. While in the bank, keep account numbers and other data out of sight, and avoid stating account numbers, Social Security numbers and similar information out loud. When planning a bank visit, have items such as deposits and withdrawal slips prepared in advance.

- Account for your interactions with vendors. Every time you speak to someone with whom you do business, write down the time, date, name and the purpose or outcome of the call. If an identity theft occurs on the vendor's end, you will be able to reference these prior conversations effectively. Be sure to note any animosity or reluctance from the vendor.

- Don't carry around your birth certificate or Social Security card. Unless it's necessary, keep those vital items in a safe, or at least a firebox. If you know someone is going to need a

copy of your tax returns or your driver's license, for example, make the copies ahead of time. This avoids the need for a firm's employee to leave the room with such information.

Of course, you can greatly reduce being a victim of such recent hacks that occurred at the major retailers by using cash more often. But if you're going to use credit, use a card from a national bank or a national credit union and never a debit card, no exceptions.

Scott A. Merritt is the CEO of Merritt Ventures Inc. and author of "Identity Theft Do's and Don'ts."