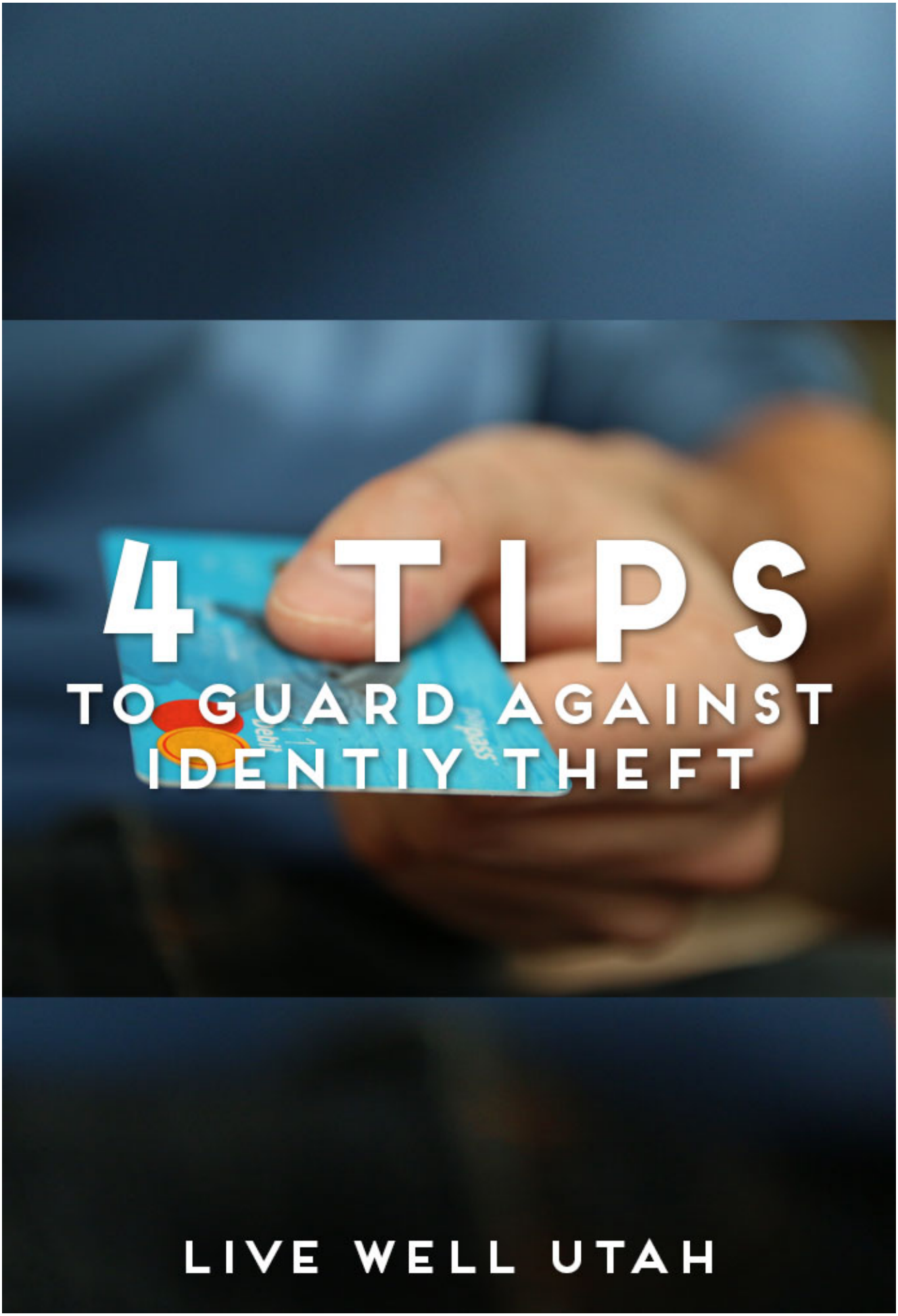
4 Tips to Guard Against Identity Theft


4 TIPS
TO GUARD AGAINST
IDENTIY THEFT
LIVE WELL UTAH

Worried about protecting your identity and keeping your personal information secure? Try these four tips from Amanda Christensen.

Sadly, it's not a matter of "if" anymore, it's more likely a matter of "when" your personal information is compromised, and in light of the recent Equifax breach there's been much buzz about what to do to protect personal information that may have been stolen. Whether your info was taken or not, this won't be the last time hackers access personal information from a "secure" site. Here are four tips to protect personal information and try to prevent the headache and heartache that identity theft brings.

Tip 1: Place a Fraud Alert on Your Credit File.

Putting a fraud alert on your credit file means businesses must try to verify your identity before extending any new credit. For example, they may call you to verify that you're the one soliciting credit from a particular business. This can make it harder for an identity thief to open an account in your name. There are a few different types:

- An "initial fraud alert" lasts 90 days and must be renewed or it will expire.
- An "extended fraud alert" lasts 7 years and is recommended for those who are victims of fraud/ID theft.
- An "active duty military alert" lasts 1 year and is intended for those in the military who want to minimize their risks while they are deployed.

It's free, and all you have to do is contact one of the three major credit reporting bureaus by phone or online. That bureau

is required to notify the other two credit reporting bureaus for you! The best part—you don't have to be a victim of ID theft to use a fraud alert.

Tip 2: Place a Credit Freeze on Your Credit File.

Unlike a fraud alert, a credit freeze prevents anyone—*including you*—from accessing your credit report information to open new accounts. Once a credit freeze is set up, you'll get a PIN number to use each time you want to freeze and unfreeze your account to apply for new credit. A credit freeze does not affect your credit score. You'll still need to monitor all bank, credit card and insurance statements for fraudulent transactions. A credit freeze lasts until you temporarily or permanently remove it. Costs range from $5-10 each time you freeze/unfreeze your credit. Finally, you must contact each of the three credit reporting bureaus individually to set up a credit freeze.

Consider this: Credit freezes can be a strong tool to protect your credit but they many not be right for everyone. Consider the cost and hassle and whether or not you plan to apply for a car loan, mortgage, student loan, etc., in the near future. If you won't need new credit anytime soon or if you've already been a victim of fraud or ID theft, then a credit freeze may be a great safeguard.

Tip 3: Set up Your Online Social Security Account.

Everyone is talking about protecting credit information, but

we can’t forget fraud committed with Social Security Numbers such as health insurance fraud and tax ID theft. One way to protect your social security number and account is to log on to ssa.gov and create a “my Social Security” account. This account documents your Social Security earnings and taxes, allows you to request a replacement card, set up direct deposit, get a replacement Medicare card (if applicable), etc. Open your personal “my Social Security” account to take away the risk of someone else trying to create one in your name. When you set the account up, you’ll be asked to verify your identity by answering multiple questions about your personal info (addresses, accounts, loans, etc.). Each time you log in, you’ll be asked for a user name, password and then you’ll be sent a verification code to your phone or email.

Consider this: You may choose the “upgrade my security” option and put even more checks in place each time you log in. If you already have an account but haven’t signed in lately, take a moment to log in and increase the security protocols by adding a second identification method, such as address, email or cell phone.

If you know your Social Security information has been compromised, you can block electronic and telephone access to your records. This means no one—INCLUDING YOU—will be able to see or change your personal info. If you decide to unblock, you will need to contact the SSA and prove your identity.

Tip 4: Be Vigilant.

Protecting personal identifiable information is not a one-and-done type situation. After you’ve taken steps like those mentioned above, you must continue to be vigilant:

- Check credit reports regularly for suspicious activity.
- File your tax return as early as possible. Don’t give an

identity thief all that time to file in your name and claim your return.

- Read EOB’s from health insurance to make sure all treatments are yours.

Remember: It’s probably not “if” it’s “when,” so be ahead of the game when protecting your personal information.

Find further information at the Consumer Protection Bureau website: consumer.ftc.gov

---

This article was written by Amanda Christensen, Extension Assistant Professor for Utah State University. Follow her on Twitter: @FamFinPro, Facebook: Fam Fin Pro, Instagram: @FamFinPro.