ID Theft Prevention

ID Theft Prevention Tips

1. Sign up for a fraud alert, or better yet a credit freeze, on your credit files at all 3 credit bureaus; sign up for a credit monitoring service; include your kids.
2. Be careful with all passwords. The best passwords are unique, long, and are not reused. Do not use dictionary words or standard number substitutions. (P455w0rd will not fool cracking tools!)
3. Be especially careful with passwords on financial accounts (obviously), social networking accounts and web-based email accounts – use unique passwords on those accounts.
4. Enable two-factor authentication whenever it is offered (e.g., Gmail). If someone attempts to log into your account from a strange or new location or device, they will be required to enter an additional code, which will be texted only to your phone.
5. Do not use the same username over multiple accounts (e.g., first initial, last name). Otherwise, hackers targeting one account may easily guess your username for another.
6. Consider using a separate and secure email address solely for password recoveries. If hackers know where your password reset is sent, you are vulnerable.
7. Back up your data regularly. If hackers gain access to your accounts, they may permanently delete your files, photos, and other important information.
8. Find out if your benefits carriers use your SSN as your ID number. If they do, ask to have it changed.
9. Check your benefits cards in your wallet for your SSN, or even its last 4 digits – If it is there, ask for a new card that omits the number.
10. Read the Explanation of Benefits received from medical insurance companies – look for unfamiliar services rendered.
11. Change your mother's maiden name with financial institutions. Use a second password instead.
12. Do not use your mother's maiden name as the answer to a security question. It is easy to discover. Consider using a fake name or word you can easily remember.

13. Consider not including last names of relatives of deceased in family obituaries (they reveal mother's maiden name).

14. Find out what information data aggregators (e.g. Choicepoint) have about you. Opt out of their databases if you see fit.

15. Check your annual Social Security Administration statements – see if someone is using your SSN to be employed.

16. Use web site security questions wisely – consider an answer that is not the real answer, but that you will remember.

17. Watch out for phishing, which involves mimicking a familiar site and asking users to enter login or personal information. Look closely at the domain name of any site before entering your data. Even if the domain name is right, it could be spoofed, so verify emails that seem suspicious.

18. Be careful with your credit card information. Only store your credit card number at a few e-commerce sites that are reputable and you use often. Even the last four digits of your card number can be used by a skilled identity thief.

19. Check credit card statements for transactions you don't recognize.

20. Shred sensitive documents before disposing of them.

21. Shop only on secure websites (look for the image of the lock at the bottom of your browser).

Contact:

Kristen J. Mathews
Head of Privacy & Data Security Group
212.969.3265
kmathews@proskauer.com

Proskauer