ATTORNEY'S ADVICE-----NO CHARGE

A corporate attorney sent the following out to the employees in his company.

1. The next time you order checks have only your initials (instead of first name) and last name put on them. If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks.

2. Do not sign the back of your credit cards. Instead, put "PHOTO ID REQUIRED."

3. When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the "For" line. Instead, just put the last four numbers. The credit card company knows the rest of the number, and anyone who might be handling your check as it passes through all the check-processing channels will not have access to it.

4. Put your work phone # on your checks instead of your home phone. If you have a PO Box, use that instead of your home address. If you do not have a PO Box, use your work address. Never have your SS# printed on your checks, (DUH!). You can add it if it is necessary. However, if you have it printed, anyone can get it.

5. Place the contents of your wallet on a photocopy machine. Do both sides of each license, credit card, etc. You will know what you had in your wallet and all of the account numbers and phone numbers to call and cancel. Keep the photocopy in a safe place. Also carry a photocopy of your passport when traveling either here or abroad. We have all heard horror stories about fraud that is committed on us in stealing a name, address, Social Security number, credit cards.

6. When you check out of a hotel that uses cards for keys (and they all seem to do that now), do not turn the "keys" in. Take them with you and destroy them. Those little cards have on them all of the information you gave the hotel, including address and credit card numbers and expiration dates. Someone with a card reader, or employee of the hotel, can access all that information with no problem whatsoever.

Unfortunately, as an attorney, I have first hand knowledge because my wallet was stolen last month. Within a week, the thieves ordered an expensive monthly cell phone package, applied for a VISA credit card, had a credit line approved to buy a Gateway computer and received a PIN number from DMV to change my driving record information online. Here is some critical information to limit the damage in case this happens to you or someone you know:

1. We have been told we should cancel our credit cards immediately. The key is having the toll free numbers and your card numbers handy so you know whom to call. Keep those where you can find them.

2. File a police report immediately in the jurisdiction where your credit cards, etc., were stolen. This proves to credit providers you were diligent, and this is a first step toward an investigation (if there ever is one). However, here is what is perhaps most important of all (I never even thought to do this.)

3. Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. I had never heard of doing that until advised by a bank that called to tell me an application for credit was made over the Internet in my name. The alert means any company that checks your credit knows your information was stolen, and they have to contact you by phone to authorize new credit. By the time I was advised to do this, almost two weeks after the theft, all the damage had been done. There are records of all the credit checks initiated by the thieves' purchases,none of which I knew about before placing the alert. Since then, no additional damage has been done, and the thieves threw my wallet away this weekend (someone turned it in). It seems to have stopped them dead in their tracks.

Now, here are the numbers you always need to contact about your wallet and contents being stolen:

1.) Equifax: 1-800-525-6285
2.) Experian (formerly TRW): 1-888-397-3742
3.) TransUnion: 1-800-680-7289
4.) Social Security Administration (fraud line): 1-800-269-0271