**NYS ATTORNEY GENERAL SCHNEIDERMAN'S TIPS FOR DATA SECURITY**

Following a reported online security breach in which hackers stole over 1 billion unique user names and passwords and half a billion e-mail addresses, New York State Attorney General Eric Schneiderman offered tips to consumers for safeguarding sensitive personal information online.  
  
This latest breach, perhaps the largest ever of its kind, targeted websites of both large and small companies as well as individuals. It is believed that individuals suspected of being responsible for such breaches sell stolen data to third parties on the black market and use the information to send spam advertisements to consumers.   
  
If you believe that you are a victim of this or any other security breach, Attorney General Schneiderman offers the following tips:  
   
• Create an identity theft fraud report. To do this, file a complaint with the Federal Trade Commission and print your Identity Theft Affidavit. You can call the FTC at (877) 438-4338 or [click here](http://www.consumer.ftc.gov/articles/0277-create-identity-theft-report" \t "_blank).  
• Use that affidavit to file a police report and create your Identity Theft Report.  
• An Identity Theft Report will help you deal with credit reporting companies, debt collectors and any fraudulent accounts that the identity thief opened in your name.  
• Put a freeze on your credit report by notifying each of the credit reporting agencies (Equifax, TransUnion or Experian). This will block someone from obtaining credit using your name or personal information. You won’t be able to apply for any new credit cards or loans while the freeze is in effect, but you can continue to use your existing cards. To freeze your credit file, you must notify each of the three major credit bureaus. You can remove the freeze temporarily or permanently by contacting each of the three agencies. There is no fee if you have been the victim of identity theft. The freeze can be removed only by you.  
• Get a copy of your credit report from each of the three agencies. You are entitled to free reports once you post a fraud alert (see below) or put a freeze on your account. Read the reports carefully to see whether other fraudulent transactions or accounts are listed, and then take steps to correct those errors.  
• Check your credit card account frequently to look for any irregular activity.  
• Change any user names and passwords. For user names and passwords, change them immediately on the relevant account and monitor the account for unusual activity. If you use the same user name or password on other accounts, change those as well.    
   
If you might be a victim:  
   
• Report to any of the three credit reporting agencies (Equifax, Transunion or Experian) that you may have been a victim of identity theft. Make sure the credit reporting agency has your current contact information so it can get in contact with you.  
• Ask the credit reporting agencies to put a fraud alert on your credit file. This will still allow you to use your credit card. If you put a fraud alert on your file, you may ask for a free credit report from each of the credit reporting agencies. Contacting any one of the three credit reporting agencies listed above is enough to file a credit alert with all of them. A credit alert must be renewed every 90 days.  
• You also have a right to put a credit freeze on your file. You may be charged a fee of up to $5 if you have not been a victim of identity theft.  
• You should also check your credit activity regularly with each credit issuer. You don’t need to wait for your monthly statement, though you should check that as well. Many banks provide online information to account holders about recent activity.  
   
The contact information for the credit reporting agencies:  
Equifax: 800-525-6285   
Experian: 888-397-3742   
TransUnion: 800-680-7289  
  
The Attorney General’s Office also suggests that consumers guard against future threats in the following ways:  
   
• Create strong passwords for online accounts and update them frequently. Use different passwords for different accounts, especially for websites where you have disseminated sensitive information, such as credit card or Social Security numbers.  
• Carefully monitor credit card and debit card statements each month. If you find any abnormal transactions, contact your bank or credit card agency immediately.  
• Do not write down or store passwords electronically. If you do, be extremely careful of where you store passwords. Be aware that any passwords stored electronically (such as in a word processing document or cell phone’s notepad) can be easily stolen and provide fraudsters with one-stop shopping for all your sensitive information. If you hand-write passwords, do not store them in plain sight.  
• Do not post any sensitive information on social media. Information such as birthdays, addresses, and phone numbers can be used by fraudsters to authenticate account information. Practice data minimization techniques. Don't overshare.  
• Always be aware of the current threat landscape. Stay up to date on media reports of data security breaches and consumer advisories.  