A SECURITY CHECK LIST: SURVIVING A DATA BREACH

Steps to take and questions to ask when personal information is lost or stolen from a company's computer system

If your credit card number or other form of information is lost or stolen from a business or government agency, that entity must notify you either by letter, e-mail or a telephone call, in most instances. In some cases, a "security breach" can result in someone using your credit card or other account number to make fraudulent purchases or transactions. Additionally, they may create new accounts under your name, which is called *Identity Theft*.

Here are some steps to take and questions to ask if you receive such a "security breach" notification:

- **Get the facts before you do anything.** The notification you receive will tell you what data was lost or stolen and when it happened. It should also provide contact information for the notifying entity so you can investigate the facts further.

- **Ask what the entity will be doing to reduce your risk of Identity Theft.** For example, will credit monitoring services be offered at no cost for a specific period of time?

- **Watch for signs of fraud.** Not every security breach ends in theft or fraud. Check your credit card billing statements for fraudulent charges and monitor your bank and other financial statements. If you spot something suspicious or unusual**,** report it to your credit card or financial company immediately.

- **Following a security breach.** Ask whether the company or agency that lost your information will notify the three major credit reporting agencies: TransUnion, Equifax and Experian. They are required to do so when more than 5,000 New Yorkers are affected.

- **Check your credit report.** Under the law, you are entitled to a free annual report from each of the three major credit reporting agencies.

Review the report carefully and follow-up with any errors or fraudulent entries.

- **Consider whether you need to close any accounts.** Depending upon the nature of the security breach, you may need to close various accounts and open new ones with password protections.

- **Learn more about personal information protections.** You may want to consider contacting a credit reporting agency and placing a “fraud alert” and “security freeze” on your credit file which will make it more difficult for someone to open a credit card account or borrow money in your name.

- **Retain your paperwork.** Keep all notes from any conversation and any records about the security breach for future reference.