CONSUMER PROTECTION ALERT

FROM
ASSEMBLYMAN
PHIL
PALMESANO
December 2013

Dear Neighbor,

Nowadays it is increasingly important to be aware of the actions you can take to protect your personal information. You should always make sure that you are receiving a fair deal and that vital information such as your social security number, credit card information, etc. is being kept safe and private.

This brochure is designed to help you become familiar with your rights as a consumer and to provide examples of practices aimed at deceiving you. It also contains information on identity theft and how to avoid becoming a victim.

If you have any questions or concerns, please contact my office.

Contact Phil
about this or other legislative matters:

Assemblyman Phil Palmesano
105 East Steuben Street
Bath, NY 14810
(607) 776-9691
palmesanop@assembly.state.ny.us

Sincerely,

Assemblyman Phil Palmesano

Important Protections for Consumers

"Freeze" Your Credit Reports

Consumers in New York State can now prohibit access - also known as "freezing" - to personal information in their credit reports to prevent identity thieves from taking out new loans and credit in their name. To place a security freeze, you must contact each of the three consumer credit reporting companies listed below and make a request in writing by certified mail or overnight mail. While you can take a freeze off your account any time, consumers should be aware that a freeze will limit a consumer's ability to get "instant credit" and it may slow credit applications.

Equifax (800) 525-6285

Experian (888) 397-3742

TransUnion (800) 680-7289

Another useful number is the Federal Trade Commission (877) 438-4338

Free Annual Credit Reports Available

You are entitled to a free copy of your credit report once every 12 months. Consumers can receive a free copy of their report from each of the credit reporting companies by visiting **www.annualcreditreport.com** or by calling their toll-free hotline at **(877) 322-8228**.

Consumer Notification

Since 2005, public and private organizations have been required to notify customers when the security of their private information has been breached in order to allow consumers to take steps to prevent their identity from being stolen or recover their information as soon as possible.

Home Improvement Protection

ESCROW ACCOUNTS

Home contracting jobs that exceed $500 must be accompanied by a written contract. In addition, any payment made on behalf of the homeowner to the contractor in excess of the cost of materials prior to the completion of the project must be deposited into an escrow account. If the job is not completed, the homeowner has the ability to recoup the deposit.

Any home improvement contractor who fails to deposit funds into an escrow account, meet additional requirements in statute or provide a written contract will be subject to a specific penalty in accordance with Article 36-A of the New York State General Business Law.

Buyer Beware

Phil Palmesano Provides Ways to Protect Yourself from Scams

Phishing Emails

Email scams remain a constant threat. So-called "Phishing" emails often try to resemble contacts you may know, so that the recipient will be comfortable opening them. The phishing scams often request personal information or ask you to click on a link. These are attempts to steal your personal information or sign you up for a paid service. To avoid these scams, you should change your passwords regularly, look for misspellings in the sender's name, email address or subject line, don't follow links without a personal message or with a blank subject line and never follow a link unless you can first verify its authenticity.

Telephone and Cell Phone Scams

Scammers have been making phone calls claiming to represent the National Do Not Call Registry. The calls claim to provide an opportunity to sign up for the registry. These calls are not coming from the Do Not Call Registry or the Federal Trade Commission, and you should not respond to them. To add your number to the **Do Not Call Registry** you can call **888-382-1222** from the phone you wish to register, or go to **https://www.donotcall.gov/register/reg.aspx** to register your home and cell phone numbers to avoid scam calls and over-the-phone soliciting.

The Money-Wiring Scam

Scammers come up with all kinds of convincing stories to get your money, from phantom lottery winnings to phony family emergencies. Many of them involve you wiring money through companies like Western Union and MoneyGram. The scammers will insist you use money transfers because it's like sending cash: the scammers get the money quickly, and you can't get it back. Typically, there's no way to reverse a transfer or trace the money, and money wired to another country can be picked up at multiple locations, so it's just about impossible to identify or track someone down. To avoid this, never send money to someone you haven't met in person and always confirm family emergencies before responding to a request for money.

Winning Contests You Never Entered

The next time you receive an unsolicited letter awarding you an expensive gift, ask yourself this: When was the last time anyone won a prize for a contest they did not enter? The truth is, these prizes are usually used to promote products like real estate or vacation time shares. You'll find the diamond you won is the size of a pinhead or the food processor is a cheap, hand-operated food chopper. You may be asked to attend a sales meeting to pick up your gift or send a shipping and handling fee. Be skeptical of unsolicited mail that is marked urgent or resembles telegrams. Never give your credit card number, Social Security number or bank account number to show eligibility or confirm an award. In short, avoid any prize that costs you time or money.

Facebook and Social Media Safety

Today, millions of Americans use Facebook and a wide array of other social media platforms to keep in touch with friends, family and colleagues, as well as explore a wide range of content. However, many users do not use, or do not know about, privacy settings that are very important to protecting personal information. Posting information about vacations or being out of town may alert criminals to an empty home and lead to burglaries. To ensure your personal information isn't falling into the wrong hands, Consumer Reports recommends nine ways to protect your information:

1. *Think before typing.*
2. *Regularly ask friends and family to check the status of your social media pages and to alert you about strange activity.*
3. *Set specific audiences for basic information like employment status or your residence.*
4. *Know what is not protected, such as profile pictures and your name.*
5. *Do not make all posts public.*
6. *Turn off "tags" so you are not automatically recognized in friends' photos.*
7. *Block apps that request to use personal information or post on your behalf.*
8. *Don't share posts with everyone, set specific people to view sensitive posts.*
9. *If you think your information may be compromised, deactivate your account.*

How to Protect your Identity

Avoid carrying excess personal information on you including extra credit cards, your social security card, birth certificate or passport.

Memorize your Debit Card PIN (personal identification number) and throw it out. Banks also recommend using your PIN only when withdrawing money from an ATM or if you want cash back while making a purchase. Otherwise use your debit card like a credit card to have extra protection against fraud.

Have your name removed from marketing lists of the three major consumer credit reporting companies: Equifax, Experian and TransUnion.

Never give your credit card number or other information over the phone unless you initiated the call and trust the business. Don't let merchants record your credit card number on a check. This is prohibited by law.

Order checks with only your initials and last name printed on them. If someone steals your checkbook, thieves will not know if you sign with your initials or name, thereby preventing fraud from occurring.

Update your computer virus programs and use a secure browser to guard the safety of your online transactions.

What Do I Do If My Identity Is Stolen?

1) *Immediately contact the fraud department at each of the three major credit bureaus and have a fraud alert placed on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts.*
2) *Order copies of your credit report and consider freezing your account.*
3) *Contact creditors for any accounts that have been tampered with or opened fraudulently. Speak to their security or fraud department to close the fraudulent account and remember to send a follow-up letter.*
4) *Contact the local police to file a report of the theft. Obtain a copy of the police report in case the credit card company or bank needs proof of the crime.*
5) *Take steps to ensure your mail, personal information and other data are protected.*

Don't download files or click on hyperlinks from strangers. Avoid "phishing" by refusing to give out personal information to companies that solicit you online. Legitimate companies do not ask for this information.

Install a lockbox at your mailbox to help reduce mail theft.

Keep a copy of your credit card numbers, account numbers, expiration dates and the telephone numbers of customer service or fraud departments in case your cards are stolen.

Use passwords on your credit card, bank accounts or phone accounts. Avoid passwords that are easily available such as birth date or last four digits of a social security number.

Cancel unused credit cards and bank accounts.

Find out who has access to your personal information at work and verify that your records are kept in a secure location.

Tear up or shred your charge receipts, copies of credit card and bank statements and expired applications or offers, checks and charge cards before throwing them out.

Stop Junk Mail

Direct mail has become a very popular tool for companies trying to gain awareness for their products. To many consumers, direct mail is junk mail. Fortunately, consumers now have the opportunity to stop junk mail from ever reaching their mailbox. The Direct Marketing Association allows consumers to sign up and take their names off direct-marketing mail lists. To sign up, go to **www.dmachoice.org** and click on "Get Started" in the upper right corner to register. Your registration will last three years and your personal information will not be shared.

Direct Marketing Association
1615 L Street
Washington, DC 20036
www.dmachoice.org

Opting-Out

Individuals also have the opportunity to "opt-out" from a variety of other types of direct marketing services through the World Privacy Forum. The top ten most popular opt-outs include:

1) **National Do Not Call Registry**
2) **Prescreened offers of credit and insurance**
3) **DMA opt-outs**
4) **Financial institution opt-outs**
5) **CAN SPAM**
6) **Credit Freeze**
7) **FERPA**
8) **Data broker opt-outs**
9) **Internet portal opt-outs**
10) **Advertising opt-outs**

No Pre-Approved Credit Cards

Pre-approving individuals with good credit has become a common solicitation tool for credit card companies to gain new customers. However, these pre-screened solicitations are an unwanted annoyance to the vast majority of consumers. Fortunately, consumers can have their names removed by visiting **www.optoutprescreen.com** and eliminate pre-approved credit card solicitations.