A Note from NYS Attorney General Letitia James

Dear New Yorkers,

Letitia James
Attorney General

Online, in the mail, even in person — your identity can be at risk.

Identity theft affects millions of people every year. Scammers assume our credit histories, grab medical benefits, even use our social security numbers for employment.

It's important to take steps to safeguard your personal information, just as you do your loved ones and personal property. Don't share your information with strangers, lock it up at home, and protect it online with strong passwords. Avoid carrying information with you when you leave home.

To find out more about how to keep your identity safe, or what to do if you believe your identity has been stolen, please go to our website: www.ag.ny.gov.

Sincerely,

Letitia James

Letitia James

New York State Attorney General
The State Capitol
Albany, New York 12224
1-800-771-7755
www.ag.ny.gov

Resources

Office of the New York State Attorney General
Consumer Frauds Bureau
800-771-7755
www.ag.ny.gov

Annual Credit Reports
www.annualcreditreport.com
877-322-8228

Major Credit Reporting Agencies
Experian
888-397-3742
www.experian.com
TransUnion:
800-888-4213
www.transunion.com
Equifax
800-685-1111
www.equifax.com
Innovis
www.innovis.com

U.S. Federal Trade Commission
877-382-4357
www.ftc.gov

PROTECT YOUR IDENTITY

NEW YORK STATE OFFICE
of the
ATTORNEY GENERAL
Consumer Frauds Bureau

KEEP YOUR IDENTITY SAFE

Secure Your Personal Information

Certain "personal identifying information" — like social security numbers, birth dates and account numbers — can give identity thieves what they need to get a credit card, a job and even medical benefits in your name. That's why it's important to guard this information carefully.

Unsolicited Calls and Mail

Never give your personal information to someone who contacts you unsolicited. Regardless of whether they call, email or approach you personally, do not give your personal information to people you don't know or did not contact.

Don't be "Phished"

Phishing is an attempt to get a victim to provide personal information such as their username, password, or credit card number. The scammers will text, email or call, indentifying themselves as your bank or a government agency. They will claim to need to "confirm your information" in order to "straighten out your account."

Legitimate financial institutions will not contact you for important information. If you are unsure, call the bank — using published numbers — to verify whether they are indeed seeking information. Don't click on links in emails from people you don't know.

Cut the Clutter

A good way to protect yourself is to reduce unsolicited offers. Here are some ways of cutting back on calls, credit card offers, and other solicitations.

TelemarketingCalls
www.donotcall.gov or 888-382-1222

Credit Card Offers
www.optoutprescreen.com or 888-567-8688

Direct Mail and Email Offers
www.dmachoice.org

Online Advertisements
www.networkadvertising.org

Social Security Number

Government agencies, employers, banking or financial institutions — there are a limited number of institutions that require your social security number. Ask why it is needed. **And, again, never give it out to someone who contacts you unsolicited.**

Limit What You Carry

Keep documents, like social security cards, at home in a safe place. Carry only the credit and bank cards you need.

Create Strong Passwords

If you use the internet, you need strong passwords, and you will need several of them. A strong password is one that:

- Cannot be easily guessed (for example your birthday, a loved one's name, a pet's name);
- Has multiple forms of characters (numbers, upper and lower case letters, symbols);
- Is at least 8 digits long;
- Is different from your other passwords.

Use passwords on:

- Wireless Internet Networks: Password your own networks; avoid conducting personal and financial business on public networks.
- Each individual computer and each account on the computer should be password protected.
- Email: if you use your email for shopping, paying bills or banking, there is a lot of personal information that can be accessed with the click of button.
- Smartphones: These are portable windows into your world. Use a strong password, in case it is lost, stolen or even borrowed by someone on the prowl.

Use Secure Websites

Secure websites "encrypt" information as it is sent. When transmitting personal or financial information look for these signs:

- **S for Secure:** Look for an "S" at the beginning of the site's name. A secured site will start with https://.
- **Security Certificate:** Many browsers use a padlock icon, others will use the site name highlighted in color before the URL (the name of the site you've signed onto). When you click on this, it will tell you the name of the owner of the certificate, which should be the same as that of the site you are on.

Destroy Unneeded Records

Shred important documents before discarding, including any record that contains personal identifying information, such as financial and medical records, receipts, tax returns, even credit card solicitations.

Monitor Statements

- Check credit card and bank statements carefully for any activity you didn't authorize.
- Medical bills and health insurance — check carefully to be sure you actually received the treatment described.

Credit Reports

Everyone is entitled to a free copy of their credit report each year, from each of the credit reporting agencies. If you see accounts or inquiries that you did not initiate or you don't recognize, it may indicate that someone else is using your identity. Request a report from each of the major credit reporting agencies. You can schedule them at different times of the year. www.annualcreditreport.com or 877-322-8228.

Child Identity Theft

Children's identities are the most commonly stolen, sometimes by family members with bad credit ratings. Protect your children's personal information as you would your own. Be sure to ask questions and take action if they receive bill collection calls or credit offers in their names, are denied benefits because someone else is using their number, or receive notices from the IRS about taxes due.