



A MESSAGE FROM ANTHONY A. SCARPINO, JR.
Westchester County District Attorney

As District Attorney, I am concerned with keeping residents in our community safe. Unfortunately, no one is immune from crime.

Identity Theft is one of the fastest growing crimes in America. This type of crime can be committed more quietly and effectively than more traditional burglaries and thefts. It can destroy years of hard work and wreak havoc with your finances. Identify Theft is a growing problem as private data becomes easier to steal. The damage done to credit ratings, bank accounts and other financial data can be particularly troublesome.

My office has a dedicated Identity Theft Unit, with specially trained Assistant District Attorneys and staff for handling these types of cases. The unit investigates and prosecutes these cases, working with victims to recover lost assets and prosecute offenders.

While we can take legal steps after a crime has taken place, preventative measures are the best way to prevent identity theft. There are steps that you can take to limit exposure and prevent yourself from becoming a victim of identity theft. This brochure will give you suggestions on how to protect your personal information and what to do in the event this type of crime has been committed against you or someone you know.

If you believe you have become the victim of Identity Theft, call the Westchester County District Attorney's Office Identity Theft Help Line at (914) 995-0002 for assistance.

Remember, vigilance is key!

Vigilance is Key

Keep an eye on your financial affairs to prevent large scale theft of your identity. Consumers are entitled to one free credit report from each of the three credit bureaus annually. Visit the web site www.annualcreditreport.com which will allow you to order your report free of charge. Look for unauthorized loans, credit card accounts opened in your name, credit inquiries that are not promotional in nature, etc.

- Shred or destroy paperwork you no longer need. Immediately report lost or stolen cards.
- Sign all credit cards upon receipt.
- Review your credit card statements carefully and immediately follow-up with creditors if bills do not arrive on time.
- Never leave your wallet or purse containing credit and debit cards in your car overnight. Be sure to lock your vehicle doors, even if your vehicle is parked in your driveway.
- Join "Fraud Alert" programs offered by your financial institutions.
- Place passwords on your credit cards, bank and phone accounts that are not obvious to others i.e. obvious passwords contain dates of birth, names, etc.
- Secure personal information in your home.
- Ensure that security procedures in the workplace protect your personal information.
- Limit the number of credit cards you carry.
- Never carry your Social Security Card with you.
- Do not give out personal information over the phone EVER!
- Bank online/pay bills online.
- Mail checks from inside the post office.

IDENTITY THEFT

Vigilance is Key!



Office of the District Attorney

RICHARD J. DARONCO COURTHOUSE
111 Dr. Martin Luther King, Jr. Blvd.
White Plains, NY 10601
(914) 995-3414
westchesterda.net



Anthony A. Scarpino, Jr.
Westchester County District Attorney

Identity theft occurs when someone uses your personal information, such as your name, Social Security number, date of birth or credit card number, without your permission, to commit fraud or other crimes. According to the Bureau of Justice Statistics, 17.6 Million US Residents experienced Identity Theft in 2014 and the number is on the rise. With sophisticated criminals constantly developing new techniques, it may not be possible or realistic to believe that you can completely prevent yourself from being victimized. If you are vigilant, however, you can educate yourself on the types of scams and if it does happen, take steps to minimize the damage to your credit.

Mail box “fishing”

Identity thieves use rodent glue traps and other mechanisms to “fish” mail from the blue United States Postal collection mailboxes. Once your mail is stolen, any personal checks might be “washed”, i.e. wiped clean of all handwriting using an acetone solution, and rewritten by the identity thief to change the payee and payment amount. The check will later be cashed or deposited and the money withdrawn. Often times the check writer won’t know for a month or more the check has gone missing. Check your bank statements frequently and report any discrepancies in written checks to your financial institution and local police department immediately. Try to place mail into receptacles located inside the post office whenever possible to minimize the risk of this fraud.

New & Existing Account Fraud

The major news networks have reported the large scale data breaches involving large financial institutions, major retailers and certain health care providers. Computer hackers and identity thieves work together to steal credit and debit card numbers and other personal identifying information such as social security numbers and dates of birth, which information can later be sold on the internet. The card numbers are

then used to create counterfeit, or “cloned” credit cards or to make internet purchases. This is how you may still be in possession of your card and yet be the victim of fraudulent card activity in another state or online. Review your credit card and bank statements frequently for unauthorized withdrawals and charges and check your credit report every four months for fraudulent account openings.

“Skimming”

When an identity thief steals credit card and debit card information as your card is processed by using a special information storage device. Keep an eye on your card. If you see your card being swiped through two different machines, contact the store manager and ask for an explanation.

17.6 Million US Residents experienced Identity Theft in 2014 and the number is on the rise.



Identity thieves seek out jobs specifically in order to get access to credit cards and other personal information or bribe bank employees to provide them with your personal and financial information.

“Spoofing”

When an identity thief chooses a domain name or email address deceptively similar to a legitimate web site or email address in order to steal private information. Make sure you double check the site address and email address to avoid being the victim of this scam. Even a discrepancy of one symbol can lead to tens of thousands of dollars in theft.

“Phishing”

When an identity thief sends an email that looks like it came from your bank or other financial institution requiring you to reply with personal information for security reasons-it may even tell you that you’ve won a prize. This is a classic identity theft scam. Do not respond. Alert your Internet service provider and financial institution.

You’ve been victimized, now what?

- Contact your local police department and file a complaint
- Contact the Westchester County District Attorney’s Office Identity Theft Help Line at (914) 995-0002
- Report the crime to the Federal Trade Commission at <https://www.ftc.gov/>
- Report fraudulent activity to your financial institution.
- Cancel your accounts and get new ones if fraudulent activity has taken place
- Notify your postal inspector if mail theft is involved.
- Contact all three credit bureaus and place a fraud alert on your credit report so that any activity will be reported to you immediately.
Equifax 1-888-766-0008 (equifax.com)
Experian 1-888-397-3742 (experian.com)
TransUnion 1(800) 680-7289 (transunion.com)

For more information

Westchester County District Attorney’s Office
westchesterda.net

Federal Trade Commission
identitytheft.gov

New York State Attorney General’s Office
ag.ny.gov

Federal Bureau of Investigation
fbi.gov

Postal Inspectors
usps.com

U.S. Secret Service
secretservice.gov