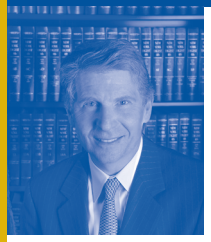
CYBERCRIME AND IDENTITY THEFT BUREAU

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE

Protecting Yourself from Identity Theft

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

5/2010



CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

Dear Friends,

Identity theft is the nation's fastest growing crime. Identity thieves steal personal information and use it to gain access to a victim's financial resources. Our office's Cybercrime and Identity Theft Bureau focuses on all aspects of this crime, including highly sophisticated criminal organizations conducting identity theft. This brochure will give you suggestions about how to protect yourself and your family from becoming victims. It also provides information about what you should do if you are a victim of identity theft. You can always call our Identity Theft Hotline at 212.335.9600 for additional help.

Sincerely,

Cyrus R. Vance, Jr.

What Is Identity Theft?

Identity theft is an increasingly common crime in which a criminal obtains your private information, such as your Social Security number or date of birth, and then fraudulently uses that information for his or her benefit. Identity theft crimes range from using a stolen credit card for a single purchase to opening multiple accounts in a victim's name. A criminal can even assume someone else's identity, most often for financial gain but sometimes in order to escape law enforcement or begin a new life.

How Do Criminals Get Your Information?

They may steal your mail or wallet, rummage through trash, hack into computers, use e-mail or telephone scams, or enlist crooked employees at companies that have legitimate access to your personal information. With relatively little information, even low-tech, inexperienced criminals can begin opening accounts in your name and running up substantial charges.

How Do I Reduce My Risk of Becoming an Identity Theft Victim?

While you can never completely protect yourself from identity theft, there are steps you can take to significantly reduce your risk of becoming a victim. In the event that you are a victim, there are a number of ways you can minimize the extent of the damage.

SHRED! SHRED! SHRED!

Before throwing documents in the garbage, shred them completely, especially those with identifying information. Cut up expired credit cards before disposing of them. Intact, discarded documents continue to be a major source of personal information used by criminals.

Never Provide Personal Information to Any Person or Company That Initiates Contact with You

Only provide information to people or companies that you have contacted directly. Beware of e-mails and phone calls requesting personal information from you, even if the source of the request is a person or company with which you are familiar.

Confirm the Need to Provide Personal Information

If a person or business asks for personal information in order to open an account or complete a transaction, confirm that such information is required. The fewer the places that have your information, the less likely it is that your information can be accessed by identity thieves.

Protect Your Social Security Number

Because a Social Security number allows access to many aspects of a person's life, it is probably the most desirable piece of information for criminals. Never provide your Social Security number unless you are 100% confident that the information is going to a legitimate, reputable organization. When possible, ask to use other types of identifiers instead. Do not carry in your wallet or purse your Social Security card or anything with your Social Security number on it. Do not print your Social Security number on personal checks.

Do Not Use Obvious Passwords or PIN Codes

PIN numbers such as your birth date, the last four digits of your Social Security number, or your mother's maiden name should not be used for access to bank accounts or to other personal information.

Keep Your Personal Information in a Secure Location

Do not leave personal information (bills, passports, or Social Security cards, for instance) lying in obvious places around your home or workplace. In the event of a break-in, you do not want burglars to be able to find your private records easily.

Protect Your Mail

Deposit all outgoing mail in a secure US Postal Service collection box. Pick up incoming mail as soon after it arrives as possible. If you are going to be out of town, either put a hold on your mail at the post office or arrange for a neighbor or friend to pick it up for you.

Cancel Any Unused Credit Cards

Having more credit cards than you need increases your exposure to identity theft. You are also less likely to regularly review the statements for unused credit cards, and as a result you may fail to pick up on suspicious transactions.

Notify the Bank of a Change of Address

If your address changes, make sure you inform any banks or credit card companies where you have accounts.

Keep Track of When Your Bills Are Received

Pay attention to when you typically receive bills. If you start noticing that your bills are arriving late or not at all, contact creditors immediately. Missing bills can be a red flag for identity theft.

Order Your Credit Reports

At least once a year, order credit reports from the three credit bureaus (see below) and look for activity that does not match up with your own records. As of September 1, 2005, all consumers throughout the United States are entitled to one free credit report per year. To receive your free credit report, you cannot contact the three nationwide credit bureaus individually; instead, you must either visit the central website for the three agencies (www.annualcreditreport.com) or call 877.322.8228. You will be given the choice to receive the report from any or all of the three nationwide credit bureaus.

Stop Unwanted Solicitations

Stop Credit Card Solicitations

Call 888.567.8688 to remove your name from lists sold to credit card companies by credit bureaus such as Equifax and Experian.

Stop Marketers' Solicitations

The Direct Marketing Association's 5,200 member companies represent 80% of direct mail marketers. To stop solicitations, complete forms online at www.the-dma.org for $5.00 or send a postcard or letter that includes your name, home address, and signature to Direct Marketing Association, Mail Preference Service, P.O. Box 643, Carmel, NY 10512.

Stop Loan Solicitations

Remove yourself from mortgage refinancing and home equity loan offers by calling the Acxiom U.S. Consumer Hotline at 877.774.2094 or writing DataQuick, Attn: Opt-Out Dept., 9620 Towne Center Drive, San Diego, CA 92121.

Activate a Security Freeze

A security freeze allows consumers to proactively put a "freeze" on their credit report. The freeze prevents credit bureaus from sharing your file with third parties, including potential creditors, without you unfreezing your file beforehand. Therefore accounts (including credit card accounts, bank loans, etc.) cannot be opened in your name without you first lifting that freeze. Beginning in November 2006, anyone who wishes to place a security freeze on his or her credit may send a written request to the credit reporting agencies. There is no cost for a first-time request or to identity theft victims. Subsequent requests to freeze or unfreeze one's credit may cost up to $5.00. To activate, a letter must be sent certified by overnight mail to each credit bureau at the following addresses.

- Equifax Security Freeze
  P.O. Box 105788, Atlanta, GA 30348
- Experian Security Freeze
  P.O. Box 9554, Allen, TX 75013
- TransUnion Security Freeze
  P.O. Box 6790, Fullerton, CA 92834-6790

The letter must include your name, address (including addresses for the past five years if you have moved in that period), Social Security number, and date of birth. If you are a victim of identity theft, you must include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If applicable, include payment by check, money order or credit card (Visa, Master Card, American Express, or Discover cards only).

Email
Do not respond to email requests from strangers.

Downloading
Never download a suspicious file or click on a hyperlink to an unfamiliar site.

Sensitive Information on the Internet
Do not send any sensitive information over the internet unless the site is secure and the recipient is a person or organization that you fully trust.

Financial Information on Your Computer
Avoid storing financial information on your computer, especially if you own a laptop. If you do keep financial records on your computer, protect this information with at least one "strong" password. Strong passwords should be at least 8 characters long and should include a combination of uppercase and lowercase letters, numbers, and symbols. You can check the strength of your password at http://www.microsoft.com/protect/fraud/passwords/checker.aspx?wt.mc_id=site_link. Do not use the auto log-in feature that allows you to access accounts without typing in a password.

Virus Protection
Update your anti-virus software on a regular basis.

Spyware Protection
Update your anti-spyware protection software on a regular basis.

Firewall
Make sure you have a firewall program installed, particularly if you use a high-speed internet connection.

Discarded Computers
Computers frequently contain a tremendous amount of personal identifying information about their users. Before you throw out a computer, use disk-wiping software that will overwrite all data on the hard drive to help ensure that no one will be able to access your files in the future.

Close Compromised Accounts

Close any accounts that have been compromised or fraudulently opened in your name.

Contact Each of the Three Major Credit Bureaus

Contact all three Credit Bureaus to request a copy of your *credit report* and place a *fraud alert* on your account.

How to Contact the Credit Bureaus

- Equifax
  www.equifax.com
  800.685.1111 (to order your credit report)
  800.525.6285 (to report fraud)
- Experian
  www.experian.com
  888.397.3742 (to order your credit report or to report fraud)
- TransUnion
  www.transunion.com
  800.888.4213 (to order your credit report)
  800.680.7289 (to report fraud)

- Credit Bureaus
  Credit bureaus are companies that provide lending institutions with credit reports on prospective borrowers. Lending institutions such as credit card companies and banks typically contact the credit bureaus before determining whether to extend credit.

- Credit Reports
  Credit reports include the prospective borrower's name, address, Social Security number and birth date; open accounts, including balances and credit limits; timeliness of payments; turnovers for collection; any suits, judgments, or tax liens; and other additional information. Reviewing a copy of your credit report will enable you to verify that no unauthorized accounts exist in your name. To receive your free annual credit report, there is a different website and phone number to use: www.annualcreditreport.com or 877.322.8228.

- Fraud Alert
  By placing a fraud alert on your account with the credit bureaus, you are requiring that the credit bureau contact you by phone (a cell phone number is suggested for convenience) when a lending institution inquires about opening a new account in your name. This way you can find out if someone other than you attempts to open accounts in your name. Then, you can take action and limit the damage to your credit history.

- Extended Fraud Alert
  This "initial" fraud alert will only last for 90 days. If you have been a victim of identity theft, you can activate an "extended" fraud alert that will last for seven years. To have an extended fraud alert placed on your credit report, you must send a letter requesting an extended alert to each credit bureau preferably by certified or overnight mail at the following addresses:

- Equifax
  P.O. Box 740241, Atlanta, GA 30374
- Experian
  P.O. Box 9532, Allen, TX 75013
- TransUnion
  P.O. Box 6790, Fullerton, CA 92834

The letter must include your name, address, Social Security number, and date of birth. In addition, a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft should be enclosed.

Call the Police

Not only can the police be helpful in catching the criminal, but they also prepare a police report that you will need to prove to creditors that you were a victim of identity fraud.

Contact the New York County District Attorney's Office Identity Theft Unit Hotline

212.335.9600.The hotline is staffed by Investigative Analysts who have expertise in prosecuting identity theft crimes and counseling victims.

Contact the Federal Trade Commission's Identity Theft Hotline

To file a complaint with the FTC, call 877.438.4338. For further information on what to do if you are a victim of identity theft, visit the FTC website: www.ftc.gov.

Contact the Internet Crime Complaint Center (IC3)

The IC3 is a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center and the Bureau of Justice Assistance. The IC3 provides a central referral mechanism for complaints involving internet related crimes. For further information on what to do if you are a victim of cybercrime, visit the IC3 website: www.ic3.gov.

Notify Any Institution Where You Have an Account

If you are unsure of the extent to which your identity has been used fraudulently, you should notify any credit card companies, banks, cell phone companies, or other businesses where you have accounts. To ensure that your professional status is not being exploited by a criminal, it is also suggested that you contact any professional organizations with which you are associated.

Contacts for Specific Types of Thefts

- **If Your Driver's License or Non-Driver's Identification Is Stolen**

  If the criminal has obtained a driver's license or non-driver's ID in your name, contact your local Department of Motor Vehicles branch.

- **If Your Social Security Number Is Being Used Fraudulently**

  You can contact the Social Security Administration's Office of the Inspector General by phone: 800. 269.0271; by fax: 410.597.0118; by mail: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235; or by e-mail: oig.hotline@ssa.gov. You can also call the Social Security Administration at 800.772.1213 to verify the accuracy of the earnings reported on your Social Security Number, to request a copy of your Social Security Statement, or to get a replacement Social Security Card if yours is lost or stolen.

- **If Your Mail Is Stolen or If a Criminal Has Fraudulently Changed Your Address**

  You can contact the U.S. Postal Inspection Service (USPIS) and report the theft to your local postal inspector. You can locate the USPIS district office nearest you by calling your local post office or checking the list at www.usps.gov/ncsc/locators/find-is.html.

- **If Your Passport Is Stolen or Lost**

  If your passport is lost, stolen, or is being used fraudulently, contact the United States Department of State (USDS) at www.travel.state.gov/passport/lost/lost_848.html or call 877.487.2778. Local field offices are listed in the Blue Pages of your telephone directory or online at www.travel.state.gov/passport/npic/agencies/agencies_913.html.

- **If a Student Loan Is Fraudulently Issued in Your Name**
  If a criminal has taken out a student loan in your name, you should close the loan by contacting the school or program that opened it. Also report the fraudulent loan to the U.S. Department of Education, which can be reached by phone at 800.MIS.USED, by email at oig.hotline@ed.gov, or by mail at the Office of Inspector General, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-1500. Visit the U.S. Department of Education at www.ed.gov/.

- **If a Tax Return Is Fraudulently Filed in Your Name**
  If a criminal is filing tax returns in your name, contact the Internal Revenue Service (IRS) at 800.829.0433. In addition, victims of identity theft who are having trouble filing their returns should call the IRS Taxpayer Advocates Office at 877.777.4778.

- **If Your Investments Have Been Compromised**
  Report this to your broker or account manager and to the SEC. You can contact the SEC via the internet at www.sec.gov/complaint.shtml, by mail at SEC Complaint Center, 100 F Street NE, Washington, DC, 20549-0213; by phone at 202.942.7040; or by fax at 703.813.6965.