



Staying Safe: Avoiding Identity Theft, Scams and Consumer Fraud

Shannon Freeman
Program Coordinator
Office of the Attorney General

At a glance...

According to the U.S. Department of Justice (Bureau of Justice Statistics):

- ▶ About 7% of persons age 16 or older were victims of identity theft in 2014.
- ▶ The majority of identity theft victims (86%) experienced the fraudulent use of existing account information, such as credit card or bank account information.
- ▶ The number of elderly victims of identity theft increased to 2.6 million in 2014.
- ▶ About 14% of identity theft victims experienced out-of-pocket losses of \$1 or more. Of these victims, about half suffered losses of more than \$100 and 14% lost \$1000 or more
- ▶ Half of identity theft victims who were able to resolve any associated problems did so in a day or less.

- Based on the 2014 Identity Theft Supplement (ITS) of the National Crime Victimization Survey (NCVS)

What is Identity Theft?

- ▶ Generally speaking, IDENTITY THEFT involves someone stealing your personal information and using it without your permission.
 - ▶ It is a serious crime that can wreak havoc with your finances, credit history, and reputation.
 - ▶ Identity theft can take time, money, and patience to resolve.
- 

Defining Identity Theft (con't)

A victim of IDENTITY THEFT may experience one or more of the following:

- ▶ unauthorized use or attempted use of an existing account, such as a credit or debit card, checking, savings, telephone, online, or insurance account (referred to as fraud or misuse of an existing account)
- ▶ unauthorized use or attempted use of personal information to open a new account, such as a credit or debit card, telephone, checking, savings, loan, or mortgage account (referred to as fraud or misuse of a new account)
- ▶ misuse of personal information for a fraudulent purpose, such as getting medical care, a job, or government benefits; renting an apartment or house; or providing false information to law enforcement when charged with a crime or traffic violation (referred to as fraud or misuse of personal information)

Consumer complaints to the FTC

According to 2014 data from the Federal Trade Commission, identity theft has topped their list of consumer complaints for the past FIFTEEN years.

Identity Theft	332,646	13%
Debt Collection	280,998	11%
Imposter Scams	276,662	11%
Telephone and Mobile Services	171,809	7%
Banks and Lenders	128,107	5%
Prizes, Sweepstakes, and Lotteries	103,579	4%
Auto-Related Complaints	88,334	3%
Shop-At-Home and Catalog Sales	71,377	3%
Television and Electronic Media	48,640	2%
Internet Services	46,039	2%

Techniques of the Identity Thief

- ▶ Phishing / Pretexting
 - ▶ Fake Job Offers
 - ▶ Skimming
 - ▶ Dumpster Diving
 - ▶ Pickpocketing and Purse-Snatching
 - ▶ Malware and Spyware
 - ▶ Fake Tax Filing
 - ▶ Change of Address
- 

Identity Theft Prevention Tips

- ▶ Don't carry your Social Security card or Medicare card in your wallet
- ▶ Be wary of requests for information by phone
- ▶ Secure your information
- ▶ Shred paperwork you don't need to keep
- ▶ Protect your computer / smart phone
- ▶ Be vigilant when traveling
- ▶ Check your credit regularly at www.annualcreditreport.com

Identity theft is a CRIME in Virginia

- ▶ An identity thief whose crime results in financial loss up to \$200 faces a misdemeanor conviction and confinement for not more than 12 months and/or a maximum fine of \$2,500.
- ▶ An identity thief, whose crime results in financial loss *greater than* \$200, faces a felony conviction and a term of imprisonment of not less than one year nor more than five years.
- ▶ For more details, please refer to [§18.2-186.3](#) of the *Code of Virginia*.

If you are a victim of identity theft...

Contact your local police or sheriff's department and file a criminal complaint



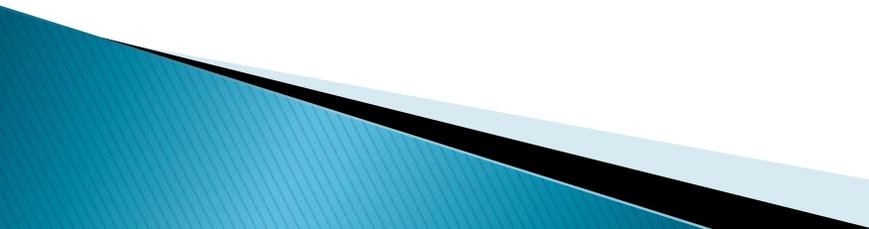
Contact the fraud units of each of the three credit bureaus (Equifax, Experian, and Trans Union) to request a fraud alert be placed on your credit report



Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge

Additionally...

You may also need to contact other agencies for other types of identity theft:

- ▶ Your local office of the [Postal Inspection Service](#) if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity
 - ▶ The [Social Security Administration](#) if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud)
 - ▶ The [Internal Revenue Service](#) if you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).
- 

Helpful Resources for Victims of Identity Theft

- ▶ Contact the [Federal Trade Commission \(FTC\)](#) to report the situation, whether online at www.consumer.ftc.gov, by telephone toll-free at 1-877-ID THEFT (877-438-4338) or TDD at 1-866-653-4261, or by mail at Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.
- ▶ Office of the Attorney General's booklet "How to Avoid Identity Theft - A Guide for Victims" and the Identity Theft Passport Program

Identity Theft Passport Program

- ▶ **What is the Attorney General's Identity Theft Passport?**

The Identity Theft Passport is a card that you can carry and present to law enforcement or other individuals who may challenge you about your identity should you become the victim of identity crime.

- ▶ **How can the Identity Theft Passport Help Me?**

The Passport is designed to serve as notification to help protect victims from unlawful detention or arrest for crimes committed by another under a stolen identity.

- ▶ **How do I get an Identity Theft Passport?**

An Identity Theft Passport may be available to any Virginian who has filed a police report because they believe they are a victim of identity crime and/or has obtained a court order expunging their record as a result of identity crime

An application for the Identity Theft Passport is available on the Attorney General's website at www.ag.virginia.gov (You must print it, complete it, sign it and mail it in.) You may also contact the Attorney General's office at 1.800.370.0459 and request an application be sent to you

Other types of fraud/scams

- ▶ Telemarketing Scams: Goods or services sold over the phone where an item either is not delivered as agreed or proves to have different qualities than described.
 - ▶ Home Improvement/Door to Door Sales Scams: Misrepresented or undelivered goods or services.
 - ▶ Advance Fee Loans/Loan Modifications: Requests that consumers (borrowers) pay a fee before obtaining promised personal loans or loan modification assistance.
- 

Types of Fraud (con't)

- ▶ Fake Check Scams: Consumers receive fake checks to pay for items (e.g., online auction), and are asked to wire part of the money back because of an “overpayment.”
- ▶ Prizes/Sweepstakes/Foreign Lottery: Deceptive promises of an award of a large sum of money, where consumer is requested to pay transfer fees or taxes upfront.

“Congratulations! You may receive a certified check for up to \$400,000,000 U.S. CASH!”

“Hundreds of U.S. citizens win every week using our secret system! You can win as much as you want!”

Telemarketing Fraud

(Tips to Protect Yourself)

- ▶ Do not be pressured to make an immediate decision.
 - ▶ Get all information in writing before you agree to make a purchase.
 - ▶ Check out any charitable organization before you decide to donate. Make sure soliciting entity is registered with the Office of Charitable and Regulatory Programs.
 - ▶ Do not give your credit card number, bank account number, or social security number to an unknown caller.
- 

National Do Not Call Registry

- ▶ If you want to stop most telemarketing calls for the sale of goods or services, consider adding your phone number to the National Do Not Call Registry administered by the Federal Trade Commission.
 - To register online, visit: www.donotcall.gov
 - To register by phone, call: 1-888-382-1222
- ▶ This will stop most but not all calls. Political organizations, charities, telephone surveyors, and any companies with which you have an existing business relationship (where you bought something, or made an inquiry within the past 18 months) can still call.
- ▶ You can ask companies with which you have existing relationship and charitable organizations to add you to their company specific do not call lists.

Lottery/Sweepstakes Fraud Prevention

- ▶ **Do not pay to collect sweepstakes winnings.**
Legitimate sweepstakes do not require you to pay “insurance,” “taxes,” or “shipping and handling charges” to collect a prize.
- ▶ **Hold onto your money.**
Do not be pressured to wire money or send by overnight delivery. Con artists will recommend these services so they can get your money before you realize you have been cheated.
- ▶ **Look-alikes are not the real thing.**
Disreputable companies sometimes use a variation of an official or nationally recognized name to try to confuse you. Insurance companies do not insure delivery of sweepstakes winnings.

Lottery Fraud (con't)

- ▶ **If you purchase a foreign lottery ticket, expect to receive many more offers for lottery or investment “opportunities.”** Your name will be placed on lists that fraudulent telemarketers buy and sell.
- ▶ **Such lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.** Although millions are confiscated, others get through. The U.S. Postal Inspection Service estimates that \$120 million is paid in response to such solicitations every year.
- ▶ **Phone numbers can deceive.** New technology can make incoming calls look as if they are coming from a nearby state or your local community. This is called “spoofing.”
- ▶ **Keep your credit card and bank account numbers to yourself.** Scam artists often ask for them during unsolicited sales and “you are a prize winner” pitches.

Just a few other scams of note...

- ▶ **E-mail Funeral Notification**

Subject: “Celebration of Your Friend’s Life Service”

We would like to offer our sincerest condolences on the passing of your dear friend. A Memorial Service will be conducted 11:00 a.m., Tuesday, July 14th, 2014. For more information, please click on the link below.

- ▶ **E-mail Court Appearance Summons**

Subject: Urgent Court Notice

You are hereby notified that you have been scheduled to appear in court. You are required to appear for this hearing on Tuesday, July 14th, 2014 at 11:00a.m. at the courthouse. Download the attached for a copy of the court notice.

The Grandparent Scam

Grandparents are scared into sending money anywhere in desperate attempts to assist a loved grandchild.

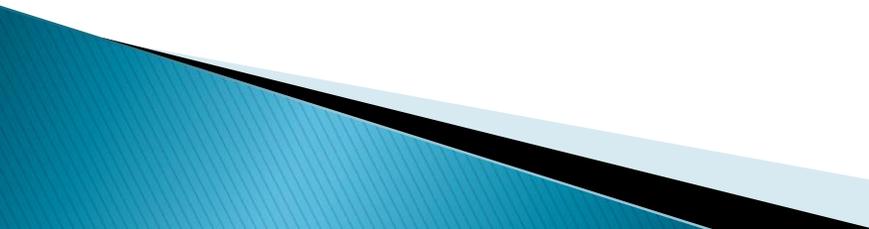
Beware of...

- Claims that your grandchild is in trouble
- Someone posing as your grandchild
- Someone speaking on behalf of your grandchild.
- Scare tactics using intimidating words (“diplomat” or “foreign attorneys”)
- Demands for monetary wire transfers
- Personal information used

Final Words on Staying Safe

- ▶ Receive a free copy of your credit report.
- ▶ Stop junk mail.
- ▶ Safeguard your personal information.
- ▶ Stop pre-approved credit card offers.
- ▶ Check home improvement services via the Virginia Board of Contractors.
- ▶ Utilize the Better Business Bureau as a resource.
- ▶ Enlist with the National Do Not Call Registry.
- ▶ Contact your phone service provider, local authorities, Federal Trade Commission or Attorney General's Office to report a scam.

If it sounds too good to be true, IT IS!



Questions?



Resources / Assistance

For more information, contact:
Office of Attorney General Mark Herring

Victim Notification Program
1.800.370.0459

Computer Crime Section
804.786.2071 / cybercrime@oag.state.va.us

Consumer Protection Section
Consumer Hotline: 800-552-9963

