How to Avoid Identity Theft

And a Guide for Victims

Office of the Attorney General of Virginia
Victim Notification Program
202 North 9th Street
Richmond, Virginia 23219

Attorney General Mark R. Herring

www.ag.virginia.gov

TABLE OF CONTENTS

HOW TO AVOID IDENTITY THEFT

Identity theft crimes are on the rise across the nation. Your personal identifying information can be accessed in a variety of ways. An imposter can misuse your information to open fraudulent credit card accounts, secure deposits on cars and housing, obtain employment opportunities, create insurance benefits, and rob retirement earnings. This form of financial sabotage can devastate your credit, and require endless hours of telephone and written communication to resolve. In the meantime, you may experience difficulty writing checks, renting apartments, and securing employment. While following these precautionary steps is not a guarantee of protection, it will greatly reduce your chances of becoming the next identity theft victim.

The rapid advance in technology in the past 50 years has created an "information revolution" that has affected government, business, commerce, education and communication. Sadly, in recent years, the increased use of computers has also led to sophisticated opportunities for criminal activity. Hardly a day goes by that the news media does not report new examples of the use of computers and the Internet to commit fraud and economic crimes such as identity theft. Thieves and con-artists often obtain an individual's personal information through e-mail and Internet scams, by going through mailboxes or trash cans for credit card receipts or calling potential victims, pretending to be on official business.

Once they have the stolen information in hand, criminals often employ computers and the Internet to quickly and easily profit from it. A thief can open accounts or purchase merchandise with a click on the computer and credit can be obtained in your name without any face-to-face interaction.

Virginia recognized the need to address this new form of crime and, in 1999, established a Computer Crime Section within the Office of the Attorney General. The Computer Crime Section is comprised of specially trained and equipped investigators and attorneys skilled in computer, communication and Internet technologies in order to vigorously investigate and prosecute illegal activities conducted over the Internet. The foremost mission of the Computer Crime Section is to assist in investigating identity theft cases and to proactively investigate and prosecute most crimes committed through the use of a computer.

If you need assistance in the investigation and/or prosecution of a computer-facilitated identity theft crime, or other computer crime, contact the Office of the Attorney General, Computer Crime Section at 804-786-2071, or at CyberCrimeUnit@oag.state.va.us.

Phishing Schemes

What Is Phishing?

Phishing (pronounced "fishing") is a computer scam criminals use to trick persons using the Internet to disclose vital financial and personal information such as Social Security numbers, account numbers, and passwords. The following is an example of a phishing scheme using e-mail:

Flounder goes on the Internet to check his e-mail. Soon, he receives an e-mail purporting to be from his bank. Although it may look authentic, the e-mail is actually a counterfeit sent by a criminal. Flounder opens the e-mail which states that his bank's security has been breached and, to protect him, his bank intends to close his account immediately, unless it can verify his account information. The e-mail requests that Flounder enter his account number and password to ensure his account remains open. Flounder takes the bait. He follows the directions in the e-mail, entering both his account number and the password to his bank account. The criminal has lured Flounder's account number and password from him. The criminal now has the ability to access Flounder's bank account.

Don't be like Flounder and take the bait! Never disclose your personal information in response to an unsolicited e-mail. If you have a question concerning a financial institution or company, call the entity directly using a verified telephone number.

What is Pharming?

Pharming (pronounced "farming") is another cyberswindle which threatens to harvest entire fields of victims. Pharmers redirect Internet users from legitimate commercial websites to counterfeit web pages to trick them to disclose their vital financial and personal information. Pharming schemes generally happen this way:

Wheat goes on the Internet intending to shop online. Wheat types in the domain name of the website where she previously shopped online. The store's website appears on her computer screen, she sees a shirt she likes and purchases it. To finalize her purchase, Wheat enters her credit card number and the expiration date. In addition, Wheat types in her home address so the shirt can be delivered to her.

Unbeknownst to Wheat, she has given her credit card number and home address to a criminal using pharming so he could harvest her financial and personal information. The criminal manipulated the domain name system (DNS) to redirect Wheat's requested website to a counterfeit website. The counterfeit website looked and operated just like the website to which Wheat intended to go.

Before you enter important personal or financial information on a webpage, verify the site's authenticity. If you know it, type in its specific IP address rather than its web name.

Does Virginia Law Protect You From Phishing and Pharming?

Yes! The Office of the Attorney General worked with the 2006 General Assembly to pass legislation aimed at curtailing pharming attacks. The new law makes it a felony to fraudulently obtain 50 or more persons' identifying information in the same occurrence with the intent to sell or distribute it. A criminal convicted of this faces up to ten (10) years imprisonment and/or up to a twenty-five hundred dollar ($2,500) fine.

Virginia law also prohibits phishing. It is a felony to use a computer to perpetrate a phishing scheme and such a crime is punishable by up to five (5) years imprisonment and/or up to a twenty-five hundred dollar ($2,500) fine for each violation. A person who uses a computer to perpetrate a phishing scheme and later sells or distributes a person's financial and personal information or uses that information to commit another crime, commits a felony punishable by up to ten (10) years imprisonment and/or a twenty-five hundred dollar ($2,500) fine.

Tips to Avoid Falling Victim to Phishing:

- Don't take the bait! Never disclose your financial or personal information in response to an unsolicited e-mail regardless of who sent it.
- Call the institution directly if you have a concern.
- Never click on a link embedded in an unsolicited e-mail, regardless of who sent it.
- Verify the authenticity of a website before entering financial or personal information via that website by using the site's certificate of authority, such as VeriSign.
- Go to a website using its specific Internet Protocol (IP) address rather than its web name.
- Check your online accounts regularly for any suspicious activity.
- Keep separate passwords for each account you have online.
- Update anti-virus software weekly.
- Install and run firewalls on your computer.

Reducing Access to Your Personal Identifying Information:

To minimize the amount of information subject to theft, do not carry extra credit cards, your Social Security card, birth certificate, or passport in your wallet or purse, except when needed.

To reduce the amount of your personal information that is in circulation, you may wish to consider the following:

- Remove your name from the marketing lists of the three credit reporting bureaus—Equifax Information Services, LLC, Experian (TRW), and TransUnion. This will limit the number of pre-approved offers of credit you receive in the mail. When tossed into the garbage, such solicitations are a potential target of identity thieves who can use them to order credit cards in your name.

- Order your credit report once a year from each of the three credit bureaus to check for inaccuracies and fraudulent use of your accounts. Go to www.annualcreditreport.com.

- Monitoring your credit card statements and your credit report are the most important steps you can take to safeguard your credit identity.

- Register your telephone number with the National Do-Not-Call Registry. This registry prevents most telemarketing calls to the registered number with the exception of calls from political organizations, charities, telephone surveyors and companies with which you have an existing business relationship.

  To register your number, visit: www.donotcall.gov
  Or, call: 1-888-382-1222

- Remove your name, home address, and home telephone number from many mailing and telephone lists through the Direct Marketing Association's Mail Preference Service and Telephone Preference Service. This free service is only available for individuals and home addresses (not businesses). You will only be removed from the Direct Marketing Association's member lists for five years, so, after five years, you need to request to be removed again.

  To remove your name and home address from national mailing lists, write to:

  DMA Mail Preference Service
  P. O. Box 643
  Carmel, NY 10512
  www.the-dma.org

- Remove your name and address from the telephone book, reverse directories, and city directories. There is usually a nominal monthly charge for this service. It typically ranges from $2 to $3 per month. By eliminating your name from these sources, you can reduce access to your personal information from sources such as the Internet (where public information resources are used as databases), telemarketers, and identity thieves. Call your local telephone service to make these changes.

- Virginia law does require you to disclose your Social Security number to the Department of Motor Vehicles when applying for a Virginia driver's license, even though it will not be on your license. The Social Security number is the most frequently used record keeping number in the United States. The widespread use of Social Security numbers makes invasion of privacy and fraud easier. Virginia law requires that a driver's license number be different than a licensee's Social Security number, unless the licensee requests in writing, that his Social Security number be used. (Virginia Code Section 46.2–323 and 342)

- Virginia law protects personal information contained within motor vehicle records from public disclosure, except in limited circumstances. (Virginia Code Section 46.2–208)

- Virginia law prohibits the State Board of Elections from releasing the Social Security number of any registered voter except on lists furnished to a court of the Commonwealth or the United States for jury selection purposes. (Virginia Code Sections 24.2–405 and 444)

- Install a locked mailbox at your residence to reduce mail theft or use a post office box.

- When you order new checks, consider removing extra information such as your Social Security number, assigned driver's license number, middle name, and telephone number. The less personal identifying information you make available, the more likely an identity thief will choose an easier target. Do not have new checks sent to your home mailbox; ask that they be delivered to the financial institution and make arrangements to pick them up.

- When you pay bills, do not leave the envelopes containing your checks at your home mailbox for the postal carrier to deliver. If stolen, your checks can be altered and then cashed. If stolen, credit card payments contain all the necessary information that an identity thief needs. To the maximum extent possible, do not write your credit card account number or Social Security number on your checks when making a payment. Virginia law generally prohibits merchants from requiring customers who pay for goods or services by check to produce a credit card for recordation of the number on the check. (Virginia Code Section 6.2–428) Due to an increased risk of theft and vandalism, it is best to mail bills, tax payments, and other sensitive items at the post office rather than from your residence or neighborhood drop boxes.

Code of Virginia

§ 18.2-186.3. Identity theft; penalty; restitution; victim assistance.

A. It shall be unlawful for any person, without the authorization or permission of the person or persons who are the subjects of the identifying information, with the intent to defraud, for his own use or the use of a third person, to:

1. Obtain, record or access identifying information which is not available to the general public that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of such other person;

2. Obtain money, credit, loans, goods or services through the use of identifying information of such other person;

3. Obtain identification documents in such other person's name;

4. Obtain, record or access identifying information while impersonating a law-enforcement officer or an official of the government of the Commonwealth.

B. It shall be unlawful for any person without the authorization or permission of the person who is the subject of the identifying information, with the intent to sell or distribute the information to another, to:

1. Fraudulently obtain, record or access identifying information that is not available to the general public that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits of such other person;

2. Obtain money, credit, loans, goods or services through the use of identifying information of such other person;

3. Obtain identification documents in such other person's name; or

4. Obtain, record or access identifying information while impersonating a law-enforcement officer or an official of the Commonwealth.

B1. It shall be unlawful for any person to use identification documents or identifying information of another person, whether that person is dead or alive, or of a false or fictitious person, to avoid summons, arrest, prosecution or to impede a criminal investigation.

C. As used in this section, "identifying information" shall include, but not be limited to: (i) name; (ii) date of birth; (iii) social security number; (iv) driver's license number; (v) bank account numbers; (vi) credit or debit card numbers; (vii) personal identification numbers (PIN); (viii) electronic identification codes; (ix) automated or electronic signatures; (x) biometric data; (xi) fingerprints; (xii) passwords; or (xiii) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain money, credit, loans goods or services.

D. Violations of this section shall be punishable as a Class 1 misdemeanor. Any violation resulting in financial loss of greater than $1,000 shall be punishable as a Class 6 felony. Any second or subsequent conviction shall be punishable as a Class 6 felony. Any violation of subsection B where five or more persons' identifying information has been obtained, recorded, or accessed in the same transaction or occurrence shall be punishable as a Class

6 felony. Any violation of subsection B where 50 or more persons' identifying information has been obtained, recorded, or accessed in the same transaction or occurrence shall be punishable as a Class 5 felony. Any violation resulting in the arrest and detention of the person whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony. In any proceeding brought pursuant to this section, the crime shall be considered to have been committed in any locality where the person whose identifying information was appropriated resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in such locality.

E. Upon conviction, in addition to any other punishment, a person found guilty of this offense shall be ordered by the court to make restitution as the court deems appropriate to any person whose identifying information was appropriated or to the estate of such person. Such restitution may include the person's or his estate's actual expenses associated with correcting inaccuracies or errors in his credit report or other identifying information.

F. Upon the request of a person whose identifying information was appropriated, the Attorney General may provide assistance to the victim in obtaining information necessary to correct inaccuracies or errors in his credit report or other identifying information; however, no legal representation shall be afforded such person.

§ 18.2-186.5. Expungement of false identity information from police and court records; Identity Theft Passport.

A. Any person whose name or other identification has been used without his consent or authorization by another person who has been charged or arrested using such name or identification may file a petition with the court for relief pursuant to § 19.2-392.2. A person who has petitioned the court pursuant to § 19.2-392.2 as a result of a violation of § 18.2-186.3, may submit to the Attorney General a certified copy of a court order obtained pursuant to § 19.2-392.2. Upon receipt by the Attorney General of a certified copy of the court order and upon request by such person, the Office of the Attorney General, in cooperation with the State Police, may issue an "Identity Theft Passport" stating that such an order has been submitted. The Office of the Attorney General shall provide access to identity theft information to (i) criminal justice agencies and (ii) individuals who have submitted a court order pursuant to this subsection.

B. Any person whose name or other identification has been used without his consent or authorization by another person may file with the Attorney General a copy of a police report showing that he has reported to a law-enforcement agency that his name or other identification has been used without his consent or authorization by another person. Upon receipt by the Attorney General of a copy of the police report and upon request by such person, the Office of the Attorney General, in cooperation with the State Police, may issue an Identity Theft Passport stating that such a police report has been submitted. The Office of the Attorney General shall provide access to identity theft information to (i) criminal justice agencies and (ii) individuals who have submitted a copy of a police report pursuant to this subsection.

C. When the Office of the Attorney General issues an Identity Theft Passport, it shall transmit a record of the issuance of the passport, and indicate under which subsection the passport was issued, to the Department of Motor Vehicles. The Department shall note on the individual's driver abstract that a court order was obtained pursuant to § 19.2-392.2 or a police report was filed and that an Identity Theft Passport has been issued. The provisions of § 2.2-3808 shall not apply to this section.

Identity Theft Protection Act

In May 2002, the Office of the Attorney General launched a statewide Identity Theft Task Force composed of technology and business leaders, law enforcement officers, legislators, identity theft victims and consumer advocates. The Task Force was charged with developing practical and effective ways to prevent identity theft and to help victims. As a result of the findings of the task force, the Virginia General Assembly enacted the Identity Theft Protection Act in 2003.

The Act provides for increased protections against identity theft including the following:

- State institutions are prohibited from displaying social security numbers on ID cards/badges. Additionally, state colleges and universities are prohibited from displaying social security numbers on student IDs. (Virginia Code Section 2.2–3808)

- Virginia law now prohibits identity theft through the impersonation of a law enforcement officer. (Virginia Code Section 18.2–186.3)

- Identity theft violations under Virginia law have been expanded to include theft of a deceased person's identity. (Virginia Code Section 18.2–186.3)

- Consumer reporting agencies are now required to note that a police report has been filed by a potential victim on that victim's credit report within 30 days of the filing of the report. (Virginia Code Section 18.2–186.3:1)

- Virginia Code Section 18.2–204.1 was amended to make it a Class 1 misdemeanor to sell or transfer a birth certificate for the purpose of identity theft. If the purpose is to acquire a firearm then it is a Class 6 felony.

- A circuit court clerk may now refuse to accept any instrument submitted for recordation that includes a grantor's, grantee's or trustee's social security number. (Virginia Code Section 17.1–227)

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.

If you have filed a police report because you are a victim of an identity crime or you have obtained an expungement order, you may apply for an Identity Theft Passport from the Office of the Attorney General. The Attorney General's Office will record and verify, with the appropriate law enforcement agency, that you have filed a police report or have obtained an expungement order. Upon verification and review of your information, the Office of the Attorney General may issue you an Identity Theft Passport stating such. The Attorney General's Office will keep a record of your application and information on file.

The Identity Theft Passport is a card you can carry and present to law enforcement or other individuals who may challenge you about your identity in the event you are the victim of identity crime. It is designed to serve as a shield to protect victims from unlawful detention or arrest for crimes committed by someone else under a stolen identity.

There are two ways to apply for the Identity Theft Passport:

Attorney General's Office:

You may fill out the Identity Theft Passport Request application located at the back of this booklet. Once completed and signed, the application should be mailed to the Attorney General's Office. In order for the Attorney General's Office to act promptly on your application, please enclose a copy of your police incident report or court order of expungement, a copy of your photo ID (copy of valid Virginia driver's license or valid DMV identification card), and any supporting documentation you may have. You may also download, print and fill out an application for an Identity Theft Passport by visiting www.ag.virginia.gov After printing, completing, and signing the Identity Theft Passport Request Form, mail it to the Attorney General's Office along with any required supporting documentation.

Or you may write to or call the Attorney General's Office for an application:

Office of the Attorney General
ID Theft Passport Program
202 North 9th Street
Richmond, VA 23219
800-370-0459

In order for your application to be complete for consideration and issuance of the Identity Theft Passport, you must include a copy of a police report filed in a Virginia jurisdiction or, if as a result of an identity crime a criminal record has been incurred in your name, you must include a copy of a court order from a Virginia court expunging your record of these criminal charges. Please include your police report or court order of expungement with your Passport application, along with a copy of your photo ID and other required supporting documentation.

Division of Motor Vehicles:

You may also complete an ID Theft Passport application provided at your local Division of Motor Vehicles ("DMV"). To apply at DMV, you cannot use the application form provided in this guide. DMV will provide you with an application form. Once completed, signed and verified, DMV will forward your application to the Attorney General's Office for processing and, if applicable, issuance of the Identity Theft Passport. DMV **ONLY** verifies your identification and forwards the application to the Attorney General's Office. DMV **does not process the application, collect from you or forward any documentation required by the Attorney General's Office** other than the completed copy of the Identity Theft Passport application. You are responsible to submit to the Attorney General's Office at the address listed above, copies of your police report, court order of expungement and any supporting documentation required to complete your application. If you have questions regarding this process, you may contact the Office of the Attorney General at the address above or call 800-370-0459.

Credit Cards

Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two of them in your wallet. Cancel all unused accounts. Even though you do not use them, their account numbers are recorded in your credit report, which is full of data that can be used by identity thieves.

Keep a list or photocopy of all of your credit cards, account numbers, expiration dates, and the telephone numbers of the customer service and fraud departments of your card issuers. Keep this list in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your cards have been lost or stolen. Do the same with your bank accounts.

Never give your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company AND YOU HAVE INITIATED THE CALL. Identity thieves have been known to call their victims with a fake story that goes something like this: "Today is your lucky day! You have been chosen by the_____ Sweepstakes to receive a free trip to the Bahamas. All we need is your credit card number and expiration date to verify you as the lucky winner."

Always take credit card and ATM receipts with you. Never toss them in a public trash container. You should also shred such receipts before discarding them in the garbage.

Request, in writing, that each of your credit card issuers removes your name from any marketing and promotional lists they may sell or share with other companies. In addition, if any of your credit card issuers send random issue convenience checks, request, in writing, to be removed from their mailing list for these checks. Credit card convenience checks are easy prey for identity thieves to steal and use, while, oftentimes, the consumer is unaware that the checks were even issued. Your credit card billing statement should contain a different address for correspondence to the issuer. Do not send your requests to the same address where you send your credit card payments.

Watch the mail when you are expecting a new credit card you have applied for or a reissued credit card that has expired. Immediately contact the issuer if the credit card does not arrive in a reasonable amount of time. Also, make sure to shred all blank credit card applications you receive in the mail that you do not use.

One of the benefits for consumers using the Internet is the ability to purchase products and services around the clock electronically from the convenience of their home or office. One of the drawbacks is the potential for fraud and deception. Be very careful before you use a credit card on the Internet or provide personal information (such as your Social Security number or date of birth) on an electronic application.

When creating passwords and PINs, do not use the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, address, or anything else that could be discovered easily by thieves.

Ask your financial institution to add extra security protection to your account. Most will allow you to use an additional code (a number or a word) when accessing your account. Do not use the common passwords and PINs listed above.

Memorize all of your passwords. Don't record them on anything in your wallet, purse, or dayplanner.

Shield your hand when using your PIN at an ATM, a debit machine, or when making long distance phone calls with your phone card. "Shoulder surfers" may be spying nearby with binoculars or a video camera.

Social Security Numbers

Protect your Social Security number. Release it only when absolutely necessary or when required by law (such as tax forms, employment records, banking/stock/property transactions, driver's/marriage/professional license applications, etc.). If a government agency requests important personal information, including your Social Security number, a Privacy Act notice should accompany the request. (5 United States Code Section 552a(e)(3)). This notice will explain whether disclosure of such information is required or requested, the use that will be made of the information, and what will happen if you refuse to provide all or any part of the information. Your Social Security number is the key to your banking accounts, credit card accounts, and your insurance and health benefits. This makes it a prime target of identity thieves. As previously discussed, you may wish to use an "assigned" driver's license number rather than your Social Security number.

Do not have your Social Security number printed on your checks. Because of the risk of fraud, even though one may be requested for identification, ask that merchants not hand-write your Social Security number on your checks. Currently, however, there is no law against a merchant requiring you to divulge your Social Security number for recordation before accepting a check. Offering an assigned driver's license number is usually an adequate substitute.

Order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) (SSA-7004) from the Social Security Administration every three years to check for inaccuracies or fraud. To request a PEBES application call or write to:

Social Security Administration
Office of Public Inquiries
Windsor Park Building
6401 Security Boulevard
Baltimore, MD 21235
Phone: 1-800-772-1213
Web site to download a PEBES application: http://www.ssa.gov

Responsible Information Handling

Carefully review your credit card statements and all of your bills for unauthorized charges or fraudulent use. Be especially careful with your phone bills, because your local telephone company is obliged to let other carriers use their billing systems for a fee. More and more, unscrupulous third parties are billing consumers for goods such as: special services, calling plans, or memberships they did not order and do not want. The practice is commonly called "cramming." Scrutinize your local, long distance, and cellular telephone bills each month for fraudulent or unauthorized charges. Additionally, be aware that some long distance telephone companies resort to deceptive tactics to switch your service without authorization. This practice is commonly called "slamming." You may contact your local telephone company to verify your long distance carrier and request a freeze on your account, which prevents account changes without your specific authorization using a password. There is often a nominal fee to "freeze" your account.

Do not toss credit card convenience checks or pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. They can be used by "dumpster divers" to cash the checks or order credit cards in your name and mail them to their address. Do the same with other sensitive information such as credit card receipts, banking statements and phone bills. Home shredders may be purchased in most office supply stores.

Demand that your financial institution adequately safeguard your personal identifying information. Discourage your bank from using the last four digits of your Social Security number as your assigned personal identification number (PIN). Request that your financial institution remove account numbers from ATM receipts (many have already done so). Inquire whether they shred all paper records before discarding them. Always take your receipts from ATMs with you and shred or store them in a safe place. By adopting responsible information handling practices, you and your financial institution can reduce the risk of fraud.

When you complete credit or loan applications, determine how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them, you may want to take your business elsewhere. Some auto dealerships, department stores, car rental agencies and video stores have been known to be careless with customer applications. For example, an employee at the business with insider access may retrieve your personal information to sell or use fraudulently. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by credit card if you think the business does not use adequate safeguards.

Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including your account number, telephone number, and driver's license number. To the extent possible, do not permit your credit card number to be written onto your checks. As a general rule and as noted above, Virginia law prohibits merchants from recording your credit card number as a condition of acceptance of a check for the sale of goods or services. Virginia law does NOT prohibit a merchant from requesting that you display a credit card, in limited situations, and for limited purposes, such as an indication of credit worthiness or identification, and, in these situations, allows the merchant to record only the card type, the issuer (bank name) and the expiration date of the credit card. However, a credit card number may be requested and recorded in lieu of a deposit to secure payment in the event of loss, damage, or default. (Virginia Code Section 6.2-428)

When in public places, always be aware of your surroundings. Thieves commonly use a distraction in cramped public places such as elevators and revolving doors to "bump and lift" your money, identification, and credit cards. Be especially cautious with bags and purses that can be an easy target for a thief to grab.

Magazines, credit card companies, clubs and organizations, charities, manufacturers, and retailers often make lists of their subscribers, customers, members, and donors available to other businesses for a fee. Because your personal information is reproduced and sold in countless ways, you should always exercise caution when making personal identifying information available on the Internet, sending a mail-in rebate/survey/warranty card, entering a drawing or sweepstakes, donating money, and even subscribing to magazine services.

A GUIDE FOR VICTIMS

It is important to act quickly and assertively to minimize damage to your credit and personal reputation. While identity theft is a crime that law enforcement officials can prosecute, the perpetrator is often difficult to track. In addition, law enforcement officials cannot clean up the havoc created for you.

In dealing with the authorities and financial institutions, keep a log of all conversations, including dates, names, and telephone numbers. Keep notes on the time spent and any expenses incurred. Confirm all conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.

Law Enforcement

Report the crime to all police and sheriff's departments with jurisdiction in your case. Depending on where the crime(s) occurred, multiple law enforcement agencies may have jurisdiction. Give them as much documented evidence as possible. Get a copy of your incident report or whatever verification the department will give you. Keep the telephone number of your fraud investigator handy and give it to creditors and others who require certification of your case. Banks and credit card companies may require you to produce the police report to verify the crime.

If you need assistance in obtaining the telephone number and address of your local sheriff, police, Commonwealth's Attorney, or a similar official of a separate Virginia city or county where the crime may have occurred, the Office of the Attorney General can assist you. The Office of the Attorney General has concurrent, or shared, jurisdiction with all Commonwealth's Attorneys to assist in the prosecution of identity theft cases throughout Virginia. For thefts that occur outside of Virginia, your local sheriff, police, or Commonwealth's Attorney may be able to assist you in locating the telephone number and address of their counterpart(s) in the other state(s). In certain cases, those officials may be able to coordinate with their counterpart(s) in the other state(s) on matters relating to the investigation and prosecution of those responsible for the thefts.

Federal and State Identity Theft Laws

The federal government and several states have passed identity theft laws. Virginia's identity theft statute is Virginia Code Section 18.2–186.3. The Federal Identity Theft and Assumption Deterrence Act is at 18 United States Code Section 1028. Federal identity theft cases are prosecuted by the United States Department of Justice.

Federal Trade Commission

The Federal Trade Commission (FTC) has a national clearinghouse for identity theft. If you are a victim, you can file a complaint with the FTC. The FTC will make your complaint available to law enforcement nationwide to assist them in their investigations and prosecutions of identity thieves. The FTC also aggregates the information in your complaint with other complaints to develop trends and statistics that enable policymakers and others to better understand identity theft and to craft effective remedies.

Federal Trade Commission
Identity Theft Clearinghouse
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
Toll-Free Hotline: 1-877-IDTHEFT (1-877-438-4338)

Credit Bureaus

Call the fraud units of the three credit reporting companies -- Equifax Information Services, LLC, Experian (TRW), and TransUnion. Report the theft of your credit cards and the misuse of your account numbers. Request that your credit account be flagged. Also, add a victim's statement (up to 100 words) to your report, such as: "My identification has been used to apply for fraudulent credit. Contact me at [your telephone number or mailing address] to verify ALL applications." Be sure to ask how long the fraud alert is posted on your credit account and how you can extend it if necessary.

Credit Bureau	Report Consumer Fraud	Request Credit Report	Get off Mailing Lists
Equifax Information Services, LLC P. O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	Call 1-888-766-0008 and write to address at left.	Call 1-800-685-1111	Call 1-888-567-8688 and write to address at left
Experian (TRW) P. O. Box 9554 Allen, TX 75013 www.experian.com	Call 1-888-397-3742	Call 1-888-397-3742	Call 1-888-567-8688
TransUnion 2 Baldwin Place P. O. Box 1000 Chester, PA 19022 www.transunion.com	Call 1-800-680-7289 and write to: Fraud Victim Asst. Dept. P. O. Box 6790 Fullerton, CA 92834-6790	Call 1-800-888-4213 or write to: P. O. Box 1000 Chester, PA 19022	Call 1-888-567-8688 and write to: TransUnion Name Removal Option P. O. Box 505 Woodlyn, PA 19094

Be aware that these measures may not entirely stop fraudulent new accounts from being opened by the identity thief. Ask the credit bureaus in writing to provide you with copies every few months so you can monitor your credit report. Upon your request, a credit bureau is required to provide you with one additional free credit report during any 12-month period, if you have reason to believe the report contains inaccurate information due to fraud. Additional credit reports shall not exceed an $11.00 charge and this fee is often waived. (15 United States Code Section 1681j(c)(3)). Request, in writing, that the credit bureaus provide you with the names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Request, in writing, that the credit bureaus remove inquiries that have been generated due to the fraudulent access. Request, in writing, that all fraudulent information and inquiries be permanently removed from your credit report. You may also request the credit bureaus to notify those who have received your credit report in the last six months to alert them to the disputed and erroneous information (two years for employers).

Creditors

Contact all creditors immediately with whom your name has been used fraudulently—by telephone and in writing. Obtain replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as "account closed at consumer's request." This is better than "card lost or stolen," because when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss. Carefully monitor your mail and credit card statements for evidence of fraudulent activity. If you find such activity, report it immediately to credit grantors.

The Federal Truth in Lending Act limits your liability, in most cases, for unauthorized credit card charges to $50.00 per card. You must notify your credit card issuers in writing. The Federal Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts. For more information on these laws, contact the FTC (see contact information under the Federal Trade Commission listed on page 12).

Request that credit grantors provide you with a copy of all fraudulent credit applications and all statements of incurred charges. Such information may be helpful in disputing the application and/or charges as fraudulent. If the credit grantor resists providing you this information, contact your local police or sheriff's department for assistance. The credit grantor should readily provide such information when requested to do so by local law enforcement authorities.

Pay particular attention to the personal identifying information the identity thief has provided on the application and note any discrepancies that may exist.

When reviewing the charges, note the date of the purchases, where the purchases were made, and what types of products or services were purchased. Look for dates, places or items that contradict your own schedule, whereabouts or tastes.

Credit Requirements to Verify Fraud

You may be asked by banks or credit grantors to complete and notarize fraud affidavits, which could become costly. The law does NOT require that a notarized affidavit be provided to banks or creditors. A written statement and supporting documentation should be sufficient (unless the bank or creditor offers to pay for the notary). Overly burdensome requirements by banks or creditors should be reported to the government authority that regulates the credit card issuer. To determine which authority regulates the particular credit card issuer in question, contact:

State Corporation Commission
Bureau of Financial Institutions
1300 East Main Street, Suite 800
P. O. Box 640
Richmond, VA 23218-0640
Phone: 1-804-371-9657
Toll Free in Virginia: 1-800-552-7945
www.scc.virginia.gov

Stolen Checks

If you have had checks stolen or bank accounts opened fraudulently, report it to the check verification companies listed below. Put stop payments on any outstanding checks if you are unsure of their validity. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account. When creating a password, do not use common numbers such as the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, address, or anything else that could easily be discovered by thieves.

Check Verification Company	Telephone Number	Mailing Address
CHEXSYSTEMS	1-800-428-9623	7805 Hudson Road, Ste. 100 Woodbury, MN 55125
CERTEGY CHECK SERVICES	1-800-237-3826	11601 N. Roosevelt Blvd. St. Petersburg, FL 33716
TELECHECK	1-800-710-9898	Headquarters: 14141 Southwest Freeway Ste. #300 Sugar Land, TX 77478

Automatic Teller Machine (ATM) Cards

If your ATM card has been stolen or compromised, contact the issuing financial institution and request a new card, account number, and password. Do not use your old password or the common passwords and personal identification numbers listed above. Under the Federal Electronic Fund Transfer Act ("EFTA"), you could lose as little as $50 and as much as all of the money taken with an ATM card, depending on when you contact the ATM card issuer in writing. For more information on the EFTA, contact the FTC (see contact information under the Federal Trade Commission listed on page 12).

Fraudulent Changes of Address, Mail Theft, or Other Mail Involvement

Notify the U.S. Postal Inspector's Office if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit bank or credit fraud. Theft of mail is a felony. Determine where the fraudulent credit cards were sent. Notify the local Postmaster for that address to forward all mail in your name to your own address. You may also need to talk with the local mail carrier for that address as well.

Criminal Investigations Service Center
ATTN: Mail Fraud
222 S. Riverside Plaza, Suite 1250
Chicago, IL 60606 - 6100
Phone: 1-877-876-2453
https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx

Secret Service Jurisdiction

The Secret Service investigates crimes dealing with credit card fraud, financial institution fraud, and crimes dealing with the false use of personal identifiers (such as name, date of birth, or Social Security number) relating to financial crimes. However, the Secret Service usually does not investigate individual cases unless the dollar amount is high or you are one of many victims of a fraud ring. If the actual crime (fraudulent application or charges) occurred outside of Virginia, the Secret Service may forward your case to the appropriate office.

U.S. Secret Service
Washington Field Office, Suite 6000
1100 L Street, N.W.
Washington, D.C. 20005
Phone: 1-202-406-8000
www.secretservice.gov

Local Information:

Norfolk 1-757-441-3200—200 Granby Street, Suite 640, Norfolk, VA 23510
Richmond 1-804-592-3086—300 Arboretum Place #500, Richmond, VA 23236
Roanoke 1-540-875-2208—105 Franklin Road, SW, Ste. 2, Roanoke, VA 24011

Social Security Number Misuse

To determine if someone is misusing your Social Security number for employment purposes, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) (SSA-7004) from the Social Security Administration to check for inaccuracies or fraud. To request a PEBES application, call or write to the office listed below. If you determine that too many or too few earnings are recorded on your PEBES, or if your name is recorded incorrectly, call or write to:

Social Security Administration/OIG Hotline
P.O. Box 17768
Baltimore, MD 21235
Phone: 1-800-269-0271
Web site to download PEBES application: http://www.ssa.gov

If someone is misusing your Social Security number, as a last resort, you may consider changing your number. The Social Security Administration will change your number only if you fit specific fraud victim criteria. For more information, call or write the office listed below and request the following fact sheet: Social Security: When Someone Misuses Your Social Security Number, SSA Pub. No. 05-10064. Report the fraudulent use of your Social Security number to:

Social Security Administration
Office of the Inspector General
P.O. Box 17768
Baltimore, MD 21235
Phone: 1-800-269-0271 (OIG Fraud/Waste/Abuse Hotline)
https://oig.ssa.gov/report

Income Tax Fraud

Any fraudulent use of another person's Social Security number, including dependents' Social Security numbers, to obtain an income tax refund should be reported to:

Internal Revenue Service
400 N. 8th Street
Richmond, VA 23219
Phone: 804-916-8700
Website: www.irs.gov/identitytheft

Virginia Department of Taxation, Identity Theft
Main Street Centre
600 East Main Street
Richmond, VA 23219
Phone: 804-404-4185
Fax: 804-344-8565
Website: www.tax.virginia.gov

U.S. Passports

If you are the victim of identity theft and have a U.S. passport, notify the U.S. Passport Agency, in writing, to be on the lookout for anyone ordering a new passport fraudulently. You should ask to have a Department of State Form #DSP-64 sent to you. This form is used to notify the Passport Agency and the State Department about the theft of your U.S. passport. You should then make a copy of that form for your records and send the original back to the agency listed on the form.

U.S. Department of State - Passport Services
Consular Lost/Stolen Passport Section
ATTN: CLASP
44132 Mercure Circle
P.O. Box 1227
Sterling, VA 20166-1227
Phone:1-877-487-2778
TTY:1-888-874-7793
www.travel.state.gov/passport

Utilities

If your cellular phone has been stolen, or if you discover fraudulent charges on your bills, cancel the accounts and open new ones. To avoid being "slammed," (deceptive tactics used to switch telephone service without authorization) request that your local telephone service freeze your long distance carrier so it cannot be changed without specific authorization from you, using a password. There is usually a nominal fee for this service. To avoid being "crammed," (being billed for special services, calling plans or memberships you do not want) scrutinize every charge on your billing statements for fraudulent or unauthorized charges. Notify your gas, electric, water, cable, and trash utilities that you are a victim of identity theft and alert them to the possibility that the thief may try to establish accounts using your personal information.

Driver's License Number Misuse

You may need to change your driver's license number if someone is using your number fraudulently. Call the Virginia Department of Motor Vehicles' Information Center and verify the last issuance date of your license. If there is a discrepancy and you have a non-commercial driver's license, go to your local driver's license station and apply for a duplicate license with an assigned number. Commercial drivers will be unable to use an assigned number, but should contact the Motor Vehicle Enforcement Office to file a fraud report. Send a letter, complete with supporting documents, requesting a fraud investigation to:

Virginia Motor Vehicle Enforcement
Operation Support Services
P.O. Box 26407
Richmond, VA 23261
Phone: 1-804-367-1678
www.dmv.state.va.us

False Civil and Criminal Judgments

Sometimes victims of identity theft are wrongfully accused of crimes committed by the imposter. If a civil judgment has been entered against you for actions taken by your imposter, contact the court, or the Commonwealth's Attorney where the judgment was entered and report that you are a victim of identity theft.

If you are wrongfully prosecuted for criminal charges, you may contact Virginia State Police at:

Virginia State Police
7700 Midlothian Turnpike
North Chesterfield, VA 23235
Phone: 1-804-674-2000

Or you may contact the Federal Bureau of Investigation and ask how to clear your name.

U.S. Federal Bureau of Investigation
J. Edgar Hoover Building
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535-0001
Phone: 1-202-324-3000

Credit Report Fraud

If you find there has been unauthorized access or use of your credit report, both this office and the Federal Trade Commission (FTC) can provide you with information about your rights under the Fair Credit Reporting Act. The FTC receives complaints from consumers who are victims of identity theft. The FTC does not investigate or prosecute criminal cases; those are handled by the United States Department of Justice. The FTC can provide information to consumers who have been victimized by identity theft to assist them in resolving financial and other problems that can result from this crime. In addition to this office, you may call or write to:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Phone: 1-202-326-2222
or 1-877-438-4338 (FTC Identity Theft Hotline)
www.ftc.gov

Insurance Coverage

You may want to consult your insurance agent to determine whether your losses are covered by household or other insurance policies.

Legal Assistance

You may want to consult a private attorney to determine what legal action to take against credit grantors and/or credit bureaus if they are not cooperative in removing fraudulent entries from your credit report or if their negligence is a factor. An attorney can help you recover from the fraud and determine whether your rights under various credit, banking, Social Security, and other laws have been violated. The Lawyer Referral Service of the Virginia State Bar can provide you with the names of attorneys in your area who handle consumer protection issues. If you should decide to consult with the attorney to whom you were referred, this service ensures that you will not be charged more than $35.00 for the first half hour of consultation. Call or write to:

Virginia State Bar
1100 East Main Street, Suite 700
Richmond, VA 23219-2800
Phone: 1-804-775-0500 or Toll Free: 1-800-552-7977

Making Changes

If you are disappointed with the privacy protection and fraud assistance available under current laws, consider writing your federal and state legislators concerning your experience. The Office of the Attorney General can assist you in obtaining their addresses and telephone numbers. Contact the Virginia Office of the Attorney General, Victim Notification Program, 202 North 9th Street, Richmond, Virginia 23219, e-mail at VNP@oag.state.va.us, visit us at www.ag.virginia.gov or call 1-800-370-0459.

Don't Give In

Remember, you are generally not responsible for any bill, portion of a bill, or checks written or cashed as a result of identity theft. Your credit rating should not be permanently affected, and no legal action should be taken against you. If any merchant, financial institution, or collection agency suggests otherwise, simply restate your willingness to cooperate, but do not allow anyone to coerce you into paying a fraudulent debt.

All Virginians should be aware of the increasingly widespread problem of identity theft. The Office of the Attorney General has produced this guide to help keep you from becoming a victim of identity theft. Should you become a victim, this guide can help you regain your good name and credit record. If you would like further information, please write to the Office of the Attorney General, Victim Notification Program, 202 North 9th Street, Richmond, Virginia 23219, e-mail at VNP@oag.state.va.us, visit us at www.ag.virginia.gov or call 1-800-370-0459.

INSTRUCTIONS FOR COMPLETING THE ID THEFT AFFIDAVIT

To make sure you do not become responsible for the debts incurred by the identity thief, you must provide proof that you didn't create the debt to each of the companies where accounts were opened or used in your name.

A working group composed of credit grantors, consumer advocates and the Federal Trade Commission (FTC) developed this ID Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

You can use this affidavit where a **new account** was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. (If someone made unauthorized charges to an **existing account**, call the company to find out what to do.)

This affidavit has two parts:

- **ID Theft Affidavit** is where you report general information about yourself and the theft.
- **Fraudulent Account Statement** is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (**NOT** originals) of any supporting documents (e.g., driver's license, police report) you have.

Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks of receiving it. Delaying could slow the investigation.

Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Please print clearly.

When you have completed the affidavit, mail a copy to each creditor, bank or company that provided the thief with the unauthorized credit, goods or services you describe. Attach to each affidavit a copy of the Fraudulent Account Statement with information only on accounts opened at the institution receiving the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. **Keep a copy of everything you submit for your records**.

If you cannot complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party.

Completing this affidavit does not guarantee the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Each of the three **National Consumer reporting agencies**. Ask each agency to place a "fraud alert" on your credit report, and send you a copy of your credit file. When you have completed your affidavit packet, you may want to send them a copy to help them investigate the disputed accounts.

   Equifax Credit Information Services, LLC
   1-888-766-0008 / 800-685-1111
   P. O. Box 740241, Atlanta, GA 30374-0241
   www.equifax.com

   Experian (TRW)
   1-888-397-3742
   P. O. Box 9554, Allen, TX 75013
   www.experian.com

   TransUnion
   1-800-680-7289 / 800-888-4213
   2 Baldwin Place
   P. O. Box 1000
   Chester, PA 19022
   www.transunion.com

2. **The fraud department at each creditor, bank or utility/service** that provided the identity thief with unauthorized credit, goods or services. This would be a good time to find out if the company accepts this affidavit, and whether they require notarization or a copy of the police report.

3. Your **local police department or sheriff's office**. Ask the officer to take a report and give you the report number and a copy of the incident report. When you have completed the affidavit packet, you may want to give them a copy to help them add to their report and verify the crime.

4. The FTC maintains the Identity Theft Data Clearinghouse -- the federal government's centralized identity theft complaint database -- and provides information to identity theft victims. You can call toll-free 1-877-ID-THEFT **(1-877-438-4338), visit www.consumer.gov/idtheft**, or send mail to:

   Identity Theft Data Clearinghouse
   Federal Trade Commission
   600 Pennsylvania Avenue, NW
   Washington, D.C. 20580

The FTC collects complaints from identity theft victims and shares their information with law enforcement nationwide. This information also may be shared with other government agencies, consumer reporting agencies, and companies where the fraud was perpetrated to help resolve identity theft-related problems.

NOTES

ID THEFT AFFIDAVIT

NAME: _____ PHONE NO. _____

Victim Information:

(1) My full legal name is

_____
(First) (Middle) (Last)(Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as:

_____
(First) (Middle) (Last)(Jr., Sr., III)

(3) My date of birth is: _____
(day/month/year)

(4) My Social Security number is ____ ____ ____ - ____ ____ - ____ ____ ____ ____

(5) My driver's license or identification card state and number are _____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(day/month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was:

_____

City _____ State _____ Zip Code _____

(9) I lived at the address in #8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (____ ____ ____) ____ _____ - ____ ____ ____ ____

My evening telephone number is (____ ____ ____) ____ _____ - ____ ____ ____ ____

How the Fraud Occurred: *(check all that apply for items 11-16)*

(11) _____ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) _____ I did not receive any benefits, money, goods or services as a result of the events described in this report.

NAME: _____ PHONE NO. _____

(13) _____ My identification documents
(for example, credit cards, birth certificate, driver's license, Social Security card, etc.) were:

_____ stolen _____ lost on or about _____.
(day/month/year)

(14) _____ To the best of my knowledge and belief, the following person(s), used my information (for example, my name, address, date of birth, existing account numbers, Social Security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

_____ _____
Name (if known) Name (if known)

_____ _____
Address (if known) Address (if known)

_____ _____
Phone Number(s) (if known) Phone Number(s) (if known)

(15) _____ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) _____ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

(Attach additional pages as necessary)

Victim's Law Enforcement Actions:

(17) (Check one) I _____ am _____ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (Check one) I _____ am _____ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (Check all that apply) I _____ have _____ have not reported the events described in this affidavit to the police or other law enforcement agency. The police _____ did _____ did not write a report.

In the event you have contacted the police or other law enforcement agency, please complete the following:

_____ _____
(AGENCY #1) (Office/Agency personnel taking report)

_____ _____
(Date of Report) (Report Number, if any)

_____ _____
(Phone Number) (E-Mail address, if any)

NAME: _____ PHONE NO. _____

Documentation Checklist:

Please indicate the supporting documentation you are able to provide to the companies you plan to notifiy. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) _____ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and do not have a photo ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) _____ Proof of residency during the time the disputed bill occurred, the loan was made, or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

(22) _____ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

_____ _____
(signature) (date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____
(signature) (printed name)

_____ _____
(date) (telephone number)

COMMONWEALTH OF VIRGINIA

COUNTY/CITY OF _____

The foregoing instrument was acknowledged before me this _____ day of _____, 20_____,

by _____.
(Name of person seeking acknowledgment)

_____
Notary Public
Notary registration number: _____
My commission expires: _____

NAME: _____ PHONE NO. _____

Fraudulent Account Statement:

Completing this Statement

- Make as many copies of this page as you need. Complete a separate page for each company you are notifying and only send it to that company. Include a copy of your signed affidavit.
- List only the account(s) you are disputing with the company receiving this form. See the example below.
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attacah a copy of that document (NOT the original).

I declare (check all that apply):

_____ As a result of the event(s) described in thte ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents.

Creditor Name/Address *(the company that opened the account or provided the goods or services*).	**Account Number**	**Type of unauthorized credit/goods/ services provided by creditor** (*if known).*	**Date issued or opened** *(if known).*	**Amount/Value provided** *(the amount charged or the cost of the goods/services).*
Example: *Example National Bank* *22 Main Street* *Columbus, Ohio 22722*	*0123456-89*	*Auto loan*	*01/05/2010*	*$25,500.00*

_____ During the time of the accounts described above, I had the following account opened with your company:

Billing name: _____

Billing address: _____

Account number: _____

Office of the Attorney General of Virginia

IDENTITY THEFT PASSPORT REQUEST -- VICTIM INFORMATION SHEET

NAME: _____
LAST FIRST MIDDLE

MAILING ADDRESS: _____
_____
_____
_____ ZIP _____

E-MAIL: _____
PHOTO ID: _____
DRIVER'S LICENSE # _____
(MUST attach copy of valid VA Driver's License or DMV ID)

PHONE: H: (____) _____ W: (____) _____
PHONE: CELL: (____) _____
DATE OF BIRTH: _____
SEX: MALE ❑ FEMALE : ❑ RACE: _____
U.S. CITIZEN: YES ❑ NO ❑
NON-U.S. CITIZEN/LAWFULLY PRESENT: YES ❑ NO ❑
PLEASE INDICATE YOUR STATUS* _____
*(*Attach copy of supporting documentation)*

SOCIAL SECURITY # _____
DATE YOU BECAME AWARE OF IDENTITY THEFT: _____
COUNTY/CITY AND STATE WHERE THEFT OCCURRED: _____
RESIDENT OF VIRGINIA AT TIME OF INCIDENT: YES ❑ NO ❑
VA LOCALITY WITH WHICH YOU FILED POLICE REPORT: _____
NAME & PHONE NUMBER OF OFFICER WHO TOOK YOUR REPORT: _____
AS A RESULT OF ID THEFT, ARE THERE CRIMINAL CHARGES ON YOUR RECORD? YES ❑ NO ❑
COPY OF VA POLICE REPORT OR EXPUNGEMENT ORDER ATTACHED (IF CRIMINAL CHARGES?) YES ❑ NO ❑
(Must provide copy of Police Report/Incident Report or Court Order/Expungement)
NAME OF COURT THAT ISSUED EXPUNGEMENT ORDER / DATE OF ORDER: _____
HAS THE PERSON WHO STOLE YOUR INFORMATION BEEN IDENTIFIED? YES ❑ NO ❑ SUSPECT NAME: _____
IF SO, HAS THE SUSPECT BEEN ARRESTED? YES ❑ NO ❑ DON'T KNOW ❑
TYPE OF THEFT / INVOLVEMENT: Credit Card ❑ SSN Misuse ❑ Driver's License ❑ Passport ❑ Stolen Checks ❑
Mail ❑ ATM ❑ Income Tax Fraud ❑ Civil/Criminal Judgment ❑ Ins. Coverage ❑ Ind. Dept. Store Acc'ts ❑ Other* ❑
(*Describe Below)

GIVE BRIEF DESCRIPTION OF THE INCIDENT(S) OF YOUR ID THEFT:

_____
_____
_____
_____

Please Read Before Signing: Please know that in accordance with § 18.2-461 it shall be unlawful for any person (i) to knowingly give a false report as to the commission of any crime to any law-enforcement official with intent to mislead, or (ii) without just cause and with intent to interfere, with the operations of any law-enforcement official. Violation of the provisions of this section shall be punishable as a Class 1 Misdemeanor.

By signing this report, I attest that the information provided above is true and accurate and I acknowledge that I did file an accurate and true police report or expungement order related to my identity theft, a copy of which is attached.

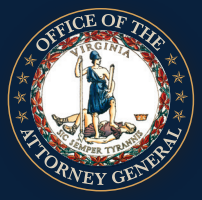
SIGNATURE: _____

DATE: _____

PLEASE INFORM THIS OFFICE IN WRITING OF ANY CHANGES IN YOUR ADDRESS

RETURN THIS FORM TO:
OFFICE OF THE ATTORNEY GENERAL
ATTN: IDENTITY THEFT PASSPORT PROGRAM
202 NORTH 9TH STREET
RICHMOND, VA 23219

PROGRAM PHONE NUMBERS:
800-370-0459
804-692-0555
804-786-0991 (FAX)



Attorney General Mark R. Herring

www.ag.virginia.gov

Office of the Attorney General of Virginia
Victim Notification Program
202 North 9th Street
Richmond, Virginia 23219
800-370-0459
Fax 804-786-0991
VNP@oag.state.va.us

"Production of this publication was supported by Grant No. 21-X9588VG19
awarded by the Virginia Department of Criminal Justice Services"

Design by the Office of Graphic Communications, Virginia Department of General Services