

ID Safety

Protecting the real you, and only you.

In partnership with:



VIRGINIA

IDENTITY THEFT RANKING BY STATE: Rank 18, 69.0 Complaints Per 100,000

Population, 5319 Complaints (2007)

Updated January 26, 2009

Current Laws: It is 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:

- 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;
- Obtain goods or services through the use of identifying information of such other person;
- Obtain identification documents in such other person's name; or
- Obtain, record, or access identifying information while impersonating a law enforcement officer or an official of the government of Virginia.

It is also 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:

- 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;
- Obtain goods or services through the use of identifying information of such other person;
- Obtain identification documents in such other person's name; or
- Obtain, record or access identifying information while impersonating a law-enforcement officer or an official of the state.

It is 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, or prosecution, or to impede a criminal investigation.

“Identifying information” includes but is not limited to: name; date of birth; Social Security number; driver’s license number; bank account numbers; credit or debit card numbers; personal identification numbers (PIN); electronic identification codes; automated or electronic signatures; biometric data; fingerprints; passwords; or any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services.

Violations are punished based on the amount of financial loss and the number of persons’ identifying information that is obtained:

- It is Class 1 misdemeanor, punishable by up to twelve months in jail and/or a fine up to \$2500, if the financial loss is less than \$200.
 - It is a Class 6 felony, punishable by one to five years in prison, or confinement in jail for up to twelve months and/or a fine up to \$2500, if the loss is greater than \$200; is a second or subsequent conviction; if five or more person's identifying information has been obtained, recorded, or accessed in the same transaction or occurrence; or if the identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation.
 - It is a Class 5 felony, punishable by one to ten years in prison, or confinement in jail for not more than 12 months and/or a fine of up to \$2500, if 50 or more persons' identifying information has been obtained, recorded, or accessed in the same transaction or occurrence
- Statute: §18.2-186.3: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3>

Jurisdiction: The crime is 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. 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.

Statute: §18.2-186.3: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3>

Statute of Limitations: State law allows prosecutions for misdemeanor identity theft to be commenced within the same limits as computer crimes. Those limits are the earlier of five years after the commission of the last illegal act or one year after the existence of the illegal act and the identity of the offender are discovered.

Statute: §19.2-8: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+19.2-8>

Phishing: State law prohibits using a computer for phishing schemes aimed at obtaining a person's financial and personal information. It is unlawful for any person to use a computer to obtain, access, or record, through the use of material artifice, trickery, or deception, any identifying information. It is a Class 5 felony to use a computer to perpetrate a phishing scheme and later sell or distribute a person's financial and personal information or use that information to commit another crime.

Statute: §18.2-152.5:1: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.5C1>

Spyware: State law prohibits any person, with malicious intent, to install or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another without the computer owner's authorization; or effect the creation or alteration of a financial instrument or of an electronic transfer of funds. Violations that collect information are a Class 6 felony. Violations involving financial instruments or transfer of funds are a Class 1 misdemeanor, unless the damage to the property of another is \$1000 or more, in which case it is a Class 6 felony. It is also a Class 6 felony if a person installs or causes to be installed computer software in violation of this section on more than five computers of another, the offense shall be a Class 6 felony.

Statute: §18.2-152.4: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-152.4>

Payment Cards: A person is guilty of credit card or credit card number theft when he:

- Takes, obtains or withholds a credit card or credit card number from the person, possession, custody or control of another without the cardholder's consent or who, with knowledge that it has been so taken, obtained or withheld, receives the credit card or credit card number with intent to use it or sell it, or to transfer it to a person other than the issuer or the cardholder;
- Receives a credit card or credit card number that he knows to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder, and who retains possession with intent to use, to sell or to transfer the credit card or credit card number to a person other than the issuer or the cardholder;
- Not being the issuer, sells a credit card or credit card number or buys a credit card or credit card number from a person other than the issuer; or
- Not being the issuer, during any twelve-month period, receives credit cards or credit card numbers issued in the names of two or more persons which he has reason to know were taken or retained under fraudulent circumstances.

Credit card or credit card number theft is grand larceny, punishable by up to twenty years in prison and/or a fine up to \$2500.

Statute: §18.2-192: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-192>

If a person, other than the cardholder or a person authorized by him, possesses two or more credit cards that are signed or two or more credit card numbers, such possession is prima facie evidence that said cards or credit card numbers were stolen.

Statute: §18.2-194: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-194>

A person is guilty of credit card forgery, a Class 5 felony, if he:

- With intent to defraud a purported issuer, a person or organization providing money, goods, services or anything else of value, or any other person, he falsely makes or falsely embosses a purported credit card or utters such a credit card;
- Not being the cardholder or a person authorized by him, with intent to defraud the issuer, or a person or organization providing money, goods, services or anything else of value, or any other person, signs a credit card; or
- Not being the cardholder or a person authorized by him, with intent to defraud the issuer, or a person or organization providing money, goods, services or anything else of value, or any other person, forges a sales draft or cash advance/withdrawal draft, or uses a credit card number of a card of which he is not the cardholder, or utters, or attempts to employ as true, such forged draft knowing it to be forged.

Statute: §18.2-193: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-193>

A person is guilty of credit card fraud if, with intent to defraud any person, he:

- Uses for the purpose of obtaining money, goods, services or anything else of value a credit card or credit card number obtained or retained unlawfully or a credit card or credit card number which he knows is expired or revoked; or
- Obtains money, goods, services or anything else of value by representing without the consent of the cardholder that he is the holder of a specified card or credit card number; or

that he is the holder of a card or credit card number and such card or credit card number has not in fact been issued.

Violations are a Class 1 misdemeanor if the value of all money, goods, services and other things of value furnished does not exceed \$200 in any six-month period; and a Class 6 felony if over \$200.

Statute: §18.2-195: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-195>

It is also a Class 6 felony to receive more than \$200 in goods and services fraudulently obtained in a six-month period. It is a Class 1 misdemeanor if under \$200.

Statute: §18.2-197: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-197>

Scanning Devices: State law prohibits the use of a scanning device or re-encoder to obtain or record encoded information from the magnetic strip of a payment card to defraud the authorized user, the issuer of the card, or a merchant. Scanning devices are defined as a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip or stripe of a payment card. A re-encoder is an electronic device that places encoded information from the magnetic strip or stripe of a payment card onto the magnetic strip or stripe of a different card. Violations are a Class 1 misdemeanor. It is a Class 6 felony if the offender later sells or distributes the information to another, or uses the information in the commission of another crime.

Statute: §18.2-196.1: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-196.1>

Social Security Number Protection: State law prohibits any government agency from requiring an individual to disclose or furnish his Social Security number (SSN), not previously disclosed or furnished, for any purpose. They also may not refuse any service, privilege or right to an individual who refuses to disclose his SSN, unless the disclosure is required by federal or state law. State law also prohibits any agency-issued identification cards, student identification cards, or license certificates to display an individuals' entire SSN.

Beginning July 1, 2009, it will be unlawful for any agency to require an individual to disclose his SSN or driver's license number unless the furnishing or disclosure of such number is authorized or required by state or federal law and essential for the performance of that agency's duties.

Victim Assistance:

Police Reports: A consumer may report a case of identity theft to the law enforcement agency in the jurisdiction where he resides.

Statute: §18.2-186.3:1: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3C1>

Restitution: Violators convicted of identity theft will be ordered to make restitution to the person whose identifying information was appropriated. This may include the person's actual expenses associated with correcting inaccuracies or errors in his credit report or other identifying information.

Statute: §18.2-186.3: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3>

Security Freeze: All Virginia consumers are allowed to place security freezes on their consumer credit reports to prevent new accounts from being opened in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, a consumer must request one in writing by certified mail or by telephone, fax, the Internet, or other electronic media if the credit reporting agency has developed procedures for consumers to do so.

The reporting agency must place the freeze within three business days after receiving the request, and within ten days of placing the request, must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the release of his credit for a specific party or period of time. However, beginning July 1, 2009, requests received by mail must be placed within one business day. Consumer reporting agencies must temporarily lift a freeze no later than 3 business days after receiving a consumer's request by mail, and no more than 15 minutes after receiving a request by an electronic contact method chosen by the consumer reporting agency. Consumer reporting agencies may charge a fee of \$10 to place the original security freeze, but victims of identity theft with a valid police report or investigative complaint may not be charged. Consumers may not be charged to temporarily unlock a freeze.

Statute: § 59.1-444.1 – 2: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+59.1-444.2>

“Credit Report Security Freeze FAQs”:

http://www.oag.state.va.us/FAQs/FAQ_CR_Security_Freeze.html

Criminal Identity Theft: 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, leading to expungement of the police and court records relating to the charge and conviction.

Statute: §19.2-392.2: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+19.2-392.2>

Credit Blocking: If a consumer submits a valid police report to a consumer reporting agency, it must block within 30 days the reporting of any information the consumer alleges is a result of the identity theft violation. The agency must promptly notify the furnisher of the information that a police report has been filed, that a block has been requested, and the effective date of the block.

Statute: §18.2-186.3:1: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.3C1>

Identity Theft Passport: Victims may apply for an identity theft passport, which can be presented to law enforcement to help prevent arrest or detention for an offense committed by another person. An identity theft passport is available to people who have filed a police report because they believe they are victims of identity crime; and/or have obtained a court order expunging their record as a result of identity crime. To obtain a passport, victims must apply through the Office of the Attorney General, which in cooperation with the State Police, will issue an Identity Theft Passport. Access to identity theft information is provided to criminal justice agencies and individuals who requested a passport.

Statute: §18.2-186.5: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+18.2-186.5>

Application: <http://www.vaag.com/FAQs/IDTPASSPORTI.pdf>

Security Breaches: State law requires businesses and state government agencies that own or license computerized data that includes personal information to disclose any breach of security of the system to any resident whose unencrypted and unredacted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notice must also be provided if encrypted information is accessed and acquired in an unencrypted form, or if the breach involves a person with access to the encryption key and individual or entity reasonably believes that the breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Personal information is defined as an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted: Social Security number; driver's license number; or a financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Notification can be provided by mail, e-mail, or telephone. If the cost of providing regular notice would exceed \$50,000, the amount of people to be notified exceeds 100,000, or the entity does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of the following: e-mail notice, conspicuous posting on the entity's web site, and notification to major statewide media. Notice must include a description of the following: the incident in general terms; the type of personal information that was subject to the unauthorized access and acquisition; the general acts of the individual or entity to protect the personal information from further unauthorized access; a telephone number that the person may call for further information and assistance, if one exists; and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

Statute: §59.1-444.2: <http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+59.1-444.2>

State Resources:

Office of the Attorney General, "How to Avoid Identity Theft – A Guide for Victims"
(<http://www.oag.state.va.us/FAQs/IDTheftBook02.pdf>)

This document directs victims to: *"Report the crime to all police and sheriff's departments with jurisdiction in your case. Depending on where the crime(s) occurred, there may be multiple law enforcement agencies having 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."*

“Identity Theft Frequently Asked Questions”

(http://www.oag.state.va.us/FAQs/FAQ_IDTheft.html)

This document directs identity crime victims to: “*First contact your local police or sheriff’s department and file a criminal complaint.*” It also directs victims to file a report with the Internet Crime Complaint Center if the crime occurred while using the Internet.

Legislation:

2008:

SB 576 / HB 1311 allows all Virginia consumers to place freezes on their credit reports. A credit freeze is a tool for victims or potential victims of identity theft to lock out inquiries into their credit report for new accounts. The fee for the freeze will be \$10, but consumers may not be charged to temporarily unlock a freeze.

Under **SB 132**, it will be unlawful for any state or local government agency to require an individual to disclose his SSN or driver’s license number unless the furnishing or disclosure of such number is authorized or required by state or federal law and essential for the performance of that agency’s duties. The law takes effect on July 1, 2009.

SB 773 allows prosecutions for misdemeanor identity theft to be commenced within the same limits as computer crimes: the earlier of five years after the commission of the last illegal act or one year after the existence of the illegal act and the identity of the offender are discovered.

HB 1469 / SB 307 requires businesses and state government agencies that own or license computerized data that includes personal information to notify consumers if personal information is acquired without authorization.

2006:

HB 1141 / SB 460 makes it a Class 6 felony for an identity theft violation if five or more persons’ identifying information was obtained in the same transaction or occurrence. It makes it a Class 5 felony if fifty or more persons’ identifying information was obtained in the same transaction or occurrence. The bill does not change provisions of current law that identity theft is a Class 1 misdemeanor unless there is a financial loss greater than \$200, in which case the penalty is a Class 6 felony.

HB 1509 provides that a consumer may report a case of identity theft to the law enforcement agency where he resides. The bill also provides that upon receipt of a court order and upon request by such person, the Office of the Attorney General, in cooperation with the State Police, must issue an "Identity Theft Passport" stating that such an order has been submitted.

2005:

SB 1147 makes it a Class 6 felony, punishable by up to five years in prison, to use a computer to obtain sensitive personal or financial information. The bill makes “phishing,” which is using a computer to gather identifying information through deception, a Class 6 felony, punishable by

up to five years in prison. If the violators also sell or distribute the identifying information gained or use the information to commit another crime (such as identity theft), the crime becomes a more serious Class 5 felony.

SB 1163 updates the state's computer crimes laws to increase penalties for computer trespass and computer invasion of privacy. The computer trespass provisions target hackers, while the computer invasion of privacy law prohibits the use of a computer to examine the employment, credit, or any other financial or personal information of another person without authority. Previously, violations were Class 1 misdemeanors. Under the new law, first offenses will continue to be a misdemeanor, but the crime becomes a felony if the information is sold or distributed to another person or the information is used in the commission of a crime, such as identity theft. Subsequent violations will also be a felony. The bill also expands the definition of larceny and receipt of stolen goods to explicitly include computers, computer networks, financial instruments, computer data, computer programs, computer software, and computer services.

2003:

SB 979 increases penalties for identity theft hackers and makes it easier for victims to fix their credit. The bill increases the prison time from 10 to 20 years for convicted criminals of identity theft whose actions resulted in more than \$200 in damages. It establishes a procedure for blocking credit misinformation appearing in a credit report and expungement of false identity information in police and court records. It also requires consumer reporting agencies 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.

The bill also seeks to make it harder for criminals to steal Social Security numbers by limiting the numbers' use on state identification cards. Similarly, **HB 1593** eliminates the now optional use of Social Security numbers as driver's license numbers for licenses issued or renewed on or after July 1.

HB 2061 clarifies that the identities of dead people are protected, and that the theft of the identity of a dead person is punishable.