

MARYLAND

IDENTITY THEFT RANKING BY STATE: Rank 10, 85.8 Complaints Per 100,000
Population, 4821 Complaints (2007)
Updated January 29, 2009

Current Laws: A person may not knowingly, willfully, and with fraudulent intent possess, obtain, or help another to possess or obtain any personal identifying information of an individual, without the consent of the individual, in order to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing of value in the name of the individual.

In addition, a person may not knowingly and willfully assume the identity of another to avoid identification, apprehension, or prosecution for a crime; with fraudulent intent to get a benefit, credit, good, service, or other thing of value; or avoid the payment of debt or other legal obligation.

“Personal identifying information” means a name, address, telephone number, driver’s license number, Social Security number, place of employment, employee identification number, mother’s maiden name, bank or other financial institution account number, date of birth, personal identification number, credit card number, or other payment device number. A “payment device number” means a code, account number, or other means of account access, other than a check, draft, or similar paper instrument, that can be used to obtain money, goods, services, or anything of value, or for purposes of initiating a transfer of funds.

Violations are a felony, punishable by up to fifteen years in prison and/or a fine up to \$25,000, if the benefit, credit, good, service, or other thing that is the subject of the crime is valued at \$500 or more. If the value is less than \$500, it is a misdemeanor, punishable by up to eighteen months in prison and/or a fine up to \$5,000. If a violation is committed pursuant to a scheme or continuing course of conduct, whether from the same or several sources, the conduct may be considered one offense. The value of goods or services may be aggregated to determine whether the violation is a felony or misdemeanor. If a person assumes the identity of another to avoid identification, apprehension, or prosecution for a crime, it is a misdemeanor, punishable by up to the eighteen months in prison and/or a fine up to \$5,000.

A person may not knowingly and willfully claim to represent another person without the knowledge and consent of that person, with the intent to solicit, request, or take any other action to otherwise induce another person to provide personal identifying information or a payment device number. Violations are a misdemeanor, punishable by up to the eighteen months in prison and/or a fine up to \$5,000.

If circumstances reasonably indicate that a person’s intent was to manufacture, distribute, or dispense another individual’s personal identifying information without the individual’s consent, it is a felony, punishable by up to five years in prison and/or a fine up to \$25,000.

Statute: Criminal Law: §8.301: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-301

Jurisdiction: State law allows the prosecution of identity theft, or any crime arising out of identity theft, to take place in any county in which an element of the crime occurred or where the victim resides. Law enforcement officers may operate without regard to jurisdictional boundaries to investigate identity fraud provisions, within specified limitations. The authority may be exercised only if an act related to the crime was committed in the jurisdiction of an investigative agency or a complaining witness resides in an investigating agency's jurisdiction. Notification of an investigation must be made to appropriate law enforcement personnel. However, once an investigation is complete, detectives in one county must contact other jurisdictions in which crimes have occurred involving the same victim and request that they file charges in those jurisdictions.

Statute: Criminal Law: §8.301: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-301

False Identification: It is a misdemeanor punishable by up to two years in prison and/or a fine of \$2000 to sell, issue, offer for sale, or offer to issue an identification card or document that contains a blank space for a person's age or date of birth, a person's incorrect age or date of birth, an incorrect name, or incorrect address. Each card or document sold or issued is a crime that may be separately prosecuted.

Statute: Criminal Law: §8-302: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-302

A person may not, with fraudulent intent: possess a fictitious or fraudulently altered government identification document; display, cause, or allow to be displayed a fictitious or fraudulently altered government identification document; lend a government identification document to another or knowingly allow the use of the person's government identification document by another; or display or represent as the person's own a government identification document not issued to the person. Violations are a misdemeanor, punishable by up to six months in prison and/or a fine up to \$500.

Statute: Criminal Law: §8-303: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-303

Payment Cards: A person may not make or cause to be made, directly or indirectly, a false statement in writing about the identity of the person or of another to procure the issuance of a credit card, knowing the statement to be false and with the intent that the statement be relied on. Violations are a misdemeanor, punishable by up to eighteen months in prison and/or a fine up to \$500.

Statute: Criminal Law: §8-203: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-203

A person is guilty of credit card theft if he:

- Takes a credit card from another, or from the possession, custody, or control of another without the consent of the cardholder; or with knowledge that a credit card has been so taken, receives the credit card with the intent to use it or sell or transfer it to another who is not the issuer or the cardholder.
- Receives a credit card that the person knows was lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and retains possession of the credit card with the intent to use, sell, or transfer it to another who is not the issuer or the cardholder.

- Sells a credit card unless the person is the issuer; or buys a credit card from a person other than the issuer.
- Receives a credit card that the person knows was taken or retained fraudulently.

Violations are a misdemeanor, punishable by up to 18 months in prison and/or a fine up to \$500.
 Statute: Criminal Law: §8-204: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-204

A person may not for the purpose of obtaining money, goods, services, or anything of value, and with the intent to defraud another, use a credit card obtained or retained illegally or a credit card that the person knows is counterfeit. In addition, a person may not, with the intent to defraud another, obtain money, goods, services, or anything of value by representing without the consent of the cardholder, that the person is the holder of a specified credit card; or that the person is the holder of a credit card when the credit card had not been issued.

Statute: Criminal Law: §8-206: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-206

It is also unlawful to receive money, goods, services, or anything of value if the person knows or believes that the money, goods, services, or other thing of value was obtained illegally

Statute: Criminal Law: §8-209: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-209

If the value of all money, goods, services, and other things of value obtained exceeds \$500, it is a felony, punishable by up to fifteen years in prison and/or a fine up to \$10,000. If the value is between \$100 and \$500, it is a misdemeanor, punishable by up to eighteen months in prison and/or a fine up to \$500. If the value is below \$100, it is a misdemeanor, punishable by up to 90 days in jail and/or a fine up to \$500.

If a person violates any of these provisions as part of one scheme or a continuing course of conduct, from the same or several sources, the conduct may be considered as one violation; and the value of money, goods, services, or things of value may be aggregated in determining if the crime is a felony or a misdemeanor.

Statute: Criminal Law: §8-202: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-202

Destruction of Records: State law requires a business, when destroying a customer's records that contain personal information, to take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account the sensitivity of the records, the nature and size of the business and its operation, the costs and benefits of different destruction methods, and available technology.

Statute: Commercial Law: §14-3501 through 3508 (Must forward through the relevant sections)
http://mlis.state.md.us/asp/statutes_respond.asp?article=gcl§ion=14-3501+&Extension=HTML

Scanning Devices: State law prohibits the possession or use of a skimming device or re-encoder that is used to obtain or record encoded information from the magnetic strip of a payment card to knowingly, willingly, and with fraudulent intent to obtain a benefit, credit, good, service, or other thing of value.

Skimming 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 without the consent of the individual authorized to use the 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.

If the benefit, good, credit, service, or other thing of value has a value of \$500 or greater, violations are a felony and are punishable by up to 15 years in prison and/or a fine up to \$25,000. If the value is under \$500, it is a misdemeanor and punishable by up to 18 months in prison and/or a fine up to \$5000.

Statute: Criminal Law: §8-301: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-301

Victim Assistance:

Mandatory Police Reports: A person who knows or reasonably suspects that he is a victim of identity fraud may contact a local law enforcement agency that has jurisdiction over any part of the county in which the person lives or any part of the county in which the crime occurred. State law requires a local law enforcement agency, after being contacted by such a person, to promptly prepare and file a report of the alleged identity fraud and provide a copy of the report to the victim. The local law enforcement agency contacted by the victim may subsequently refer the matter to a law enforcement agency with proper jurisdiction. A report filed under this section is not required to be counted as an open case for purposes including compiling open case statistics.

Statute: Criminal Law: §8.304: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-304

Restitution: A person convicted of identity fraud may be ordered to make restitution to the victim for reasonable costs, including reasonable attorney's fees; or costs incurred in clearing the victim's credit history or credit rating, or in connection with a civil or administrative proceeding to satisfy a debt, lien, judgment, or other obligation of the victim that arose because of the violation.

Statute: Criminal Law: §8.301: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-301

Security Freeze: All Maryland 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. Starting January 1, 2010, consumers will be able to request a freeze by e-mail, telephone, or through a secure Internet connection. Consumer reporting agencies may charge a fee of \$5 to place or temporarily lift a security freeze. However, victims of identity theft with a report of alleged identity theft fraud or an identity theft passport may not be charged.

The reporting agency must place the freeze within three business days after receiving the request, and within five days after placing the freeze, 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. Requests for a temporary unlocking of the freeze must be completed within three business days.

Statute: Commercial Law: §14-1212.1:

http://mlis.state.md.us/asp/statutes_respond.asp?article=gcl§ion=14-1212.1&Extension=HTML

How to Place a Security Freeze in Maryland:

<http://www.consumersunion.org/pdf/security/securityMD.pdf>

Security Breach: State law requires a business that owns or licenses computerized data that includes the personal information of a Maryland resident to conduct a reasonable and prompt investigation of any breach of security to determine the likelihood that personal information has been or will be misused as a result of the breach. If, after the investigation is concluded, the business determines that misuse of an individual's personal information has occurred or is reasonably likely to occur as a result of the breach of security, the business must notify the individual of the breach. A security breach occurs upon "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by the business."

Personal information is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: Social Security number; driver's license number; a financial account number, including a credit or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or a taxpayer identification number. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Notice must be made as soon as reasonably practicable after the business conducts the investigation, but may be delayed upon the request of law enforcement or to determine the scope of the breach, identify the individuals affected, or to restore the reasonable integrity of the data system. Notification can be provided by mail, e-mail, or by telephone. If the cost of providing regular notice would exceed \$100,000, the amount of people to be notified exceeds 175,000, or the business or agency 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 all of the following, as applicable: e-mail notice, conspicuous posting on the business's web site, and notification to statewide media. If the number of affected consumers is 1,000 or more, the consumer reporting agencies must also be notified. In addition, the business must inform the Office of the Attorney General before notifying consumers.

The notification must include, to the extent possible, a description of the categories of information that were or are reasonably believed to have been acquired by an unauthorized person; contact information for the business making the notification, the major consumer reporting agencies, and the Federal Trade Commission and the Office of the Attorney General; and a statement that the individual can obtain information from these sources about steps the individual can take to avoid identity theft.

Statute: Commercial Law: §14-3501 through 3508 (Must forward through the relevant sections)
http://mlis.state.md.us/asp/statutes_respond.asp?article=gcl§ion=14-3501&Extension=HTML

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 using the person's personal identifying information. It may also be presented to a creditor to aid in the investigation of a fraudulent accounts or charges. A person who knows or reasonably suspects that he is a victim of identity theft who has filed a police report may apply for an identity theft passport through a law enforcement agency. The agency will submit the application and copy of the police report to the Office of the Attorney General for processing and issuance of the passport. A law enforcement agency or creditor that is presented with an identity theft passport has sole discretion to accept or reject the identity theft passport. In determining whether to accept or reject the identity theft passport, the law enforcement agency or creditor may consider the surrounding circumstances and available information regarding the offense of identity fraud against the person.

Statute: Criminal Law: §8-305: http://mlis.state.md.us/asp/web_statutes.asp?gcr&8-305

State Resources:

Office of the Attorney General: , “Protect Yourself from Identity Theft”
(<http://www.oag.state.md.us/idtheft/index.htm>)

“Identity Theft – What To Do If It Happens To You”
(<http://www.oag.state.md.us/idtheft/idtheft3.pdf>)

This document directs victims to: *“Report the fraudulent activity to your local police or sheriff’s department. Under Maryland law, local police have state-wide jurisdiction over identity theft crimes. Give them as much documented evidence as possible. Make sure the police report lists the fraud accounts. Get a copy of the report. Keep the phone number of the fraud investigator handy and give it to creditors and others who require verification of your case. You will need a copy of a police report to dispute fraudulent charges on existing accounts, close fraudulently-opened accounts and block fraudulent information on your credit report. If a police department refuses to take a report, contact the ID Theft Unit for help.*

It also describes what victims should do if they learn that imposters using their name were arrested or had arrest records issued against them: *“If criminal violations are wrongfully attributed to your name, contact the police department that arrested the person using your identity, or the court agency that issued the warrant for the arrest. Explain that this is a case of misidentification and that someone is using your personal information. You may need to file an impersonation report to confirm your identity. If the arrest warrant is from a state or county other than where you live, ask your local police department to send the impersonation report to the appropriate police department. In addition to correcting your record in criminal justice databases, you’ll also want to clear your name in court records. Contact the State’s Attorney’s office in the county where the case was prosecuted.”*

“How to Freeze Your Credit Report” (<http://www.oag.state.md.us/idtheft/freezing.htm>)

“About Information Security Breaches” (<http://www.oag.state.md.us/idtheft/databreech.htm>)

Commission on Financial Regulation, “Protecting Yourself Against Identity Theft” (<http://www.dllr.state.md.us/finance/identitytheft.htm>)

This document contains both prevention tips and instructions for victims. It directs victims to: “*File a report with your local police department.*”

Legislation:

2008:

Lawmakers passed a comprehensive bill (**HB 1113**) targeting identity theft. The bill:

- Increases the maximum imprisonment penalty for felony identity fraud from 5 to 15 years.
- Establishes that it is a crime for a person to intentionally, willfully, and without authorization copy, attempt to copy, possess, or attempt to possess the contents of a computer database that was unlawfully accessed.
- Prohibits a person from using a re-encoder or skimming device to access, read, or scan personal identifying information or a payment device number.

2007:

SB 52 / HB 117 allows all Maryland consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts 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.

SB 194 / HB 208 requires businesses to protect an individual’s personal information and notify a consumer if his personal information was acquired as a result of a security system breach.

HB 1036 targets pretexting, which occurs when a person falsely claims to be someone else or to represent a business and tries to obtain confidential information about another person. The bill expands the definition of identity fraud to include this practice. Under the law, a person may not knowingly and willfully claim to represent another person without the knowledge and consent of that person, with the intent to solicit, request, or take any other action to otherwise induce another person to provide personal identifying information or a payment device number. Violations are a misdemeanor, punishable by up to eighteen months in prison and/or a fine up to \$5,000.

2006:

HB 1201 authorizes an identity theft passport program for victims of the crime. Victims can present the passport to law enforcement to help prevent arrest or detention for an offense committed by another person using the passport owner’s personal identifying information. It may also be presented to a creditor to aid in the investigation of a fraudulent account that is

opened in his/her name or a fraudulent charge that is made against an account. To obtain a passport, victims must file a police report and apply through a law enforcement agency.

2005:

HB 800 requires a local law enforcement agency, after being contacted by a person who knows or reasonably suspects that he/she is a victim of identity fraud, to promptly prepare and file a report of the alleged identity fraud and provide a copy of the report to the victim.

2004:

SB 257 allows the prosecution of identity theft, or any crime arising out of identity theft, to take place in any county in which an element of the crime occurred or where the victim resides, and authorizes the Attorney General to investigate and prosecute these crimes with all the powers and duties of a State's attorney.

2003:

SB 135 significantly increases the penalties for violating Maryland's existing identity fraud and identity theft statutes. The bill increases from \$5,000 to \$25,000 the maximum fine for a person knowingly, willfully, and with fraudulent intent possessing, obtaining, or helping another person to possess or obtain any personal identifying information of an individual without consent in order to use, sell, or transfer the information to get a benefit, credit, good, service, or other thing valued at \$500 or more in the name of the individual.

2002:

HB 358 / SB 559 increases penalties for identity theft. It makes it a felony, punishable by up to five years in prison, to manufacture or distribute personal identifying information without the individual's consent. Someone using another person's information to get a benefit of more than \$500 would be punished by up to 10 years in prison. Previously, using someone else's identity was a misdemeanor punishable by a fine of up to \$5,000 or up to a year in prison. The legislation also extends the current law to make it illegal to possess personal identifying information with the intent to distribute it. It also expands police authority to operate without regard to jurisdictions, an important distinction because the victim, the criminal and the crime are often in different places.