

IL Electronic Crime Statutes

[\(http://www.ilga.gov/\)](http://www.ilga.gov/)

(720 ILCS 5/Art. 16D heading)

ARTICLE 16D.

COMPUTER CRIME

(720 ILCS 5/16D-1) (from Ch. 38, par. 16D-1)

Sec. 16D-1. Short title. This Article shall be known and may be cited as the "Computer Crime Prevention Law".

(Source: P.A. 85-926.)

(720 ILCS 5/16D-2) (from Ch. 38, par. 16D-2)

Sec. 16D-2. Definitions. As used in this Article, unless the context otherwise indicates:

(a) "Computer" means a device that accepts, processes, stores, retrieves or outputs data, and includes but is not limited to auxiliary storage and telecommunications devices connected to computers.

(a-5) "Computer network" means a set of related, remotely connected devices and any communications facilities including more than one computer with the capability to transmit data among them through the communications facilities.

(b) "Computer program" or "program" means a series of coded instructions or statements in a form acceptable to a computer which causes the computer to process data and supply the results of the data processing.

(b-5) "Computer services" means computer time or services, including data processing services, Internet services, electronic mail services, electronic message services, or information or data stored in connection therewith.

(c) "Data" means a representation of information, knowledge, facts, concepts or instructions, including program documentation, which is prepared in a formalized manner and is stored or processed in or transmitted by a computer. Data shall be considered property and may be in any form including but not limited to printouts, magnetic or optical storage media, punch cards or data stored internally in the memory of the computer.

(c-5) "Electronic mail service provider" means any person who (1) is an intermediary in sending or receiving electronic mail and (2) provides to end-users of electronic mail services the ability to send or receive electronic mail.

(d) In addition to its meaning as defined in Section 15-1 of this Code, "property" means: (1) electronic impulses; (2) electronically produced data; (3) confidential, copyrighted or proprietary information; (4) private identification codes or numbers which permit access to a computer by authorized computer users or generate billings to consumers for purchase of goods and services, including but not limited to credit card transactions and telecommunications services or permit electronic fund transfers; (5) software or programs in either machine or human readable form; or (6) any other tangible or intangible item relating to a computer or any part thereof.

(e) "Access" means to use, instruct, communicate with, store data in, retrieve or intercept data from, or otherwise utilize any services of a computer.

(f) "Services" includes but is not limited to computer time, data manipulation or storage functions.

(g) "Vital services or operations" means those services or operations required to provide, operate, maintain, and repair network cabling, transmission, distribution, or computer facilities necessary to ensure or protect the public health, safety, or welfare. Public health, safety, or welfare include, but are not limited to, services provided by medical personnel or institutions, fire departments, emergency services agencies, national defense contractors, armed forces or militia personnel, private and public utility companies, or law enforcement agencies.

(Source: P.A. 91-233, eff. 1-1-00.)

(720 ILCS 5/16D-3) (from Ch. 38, par. 16D-3)

Sec. 16D-3. Computer Tampering.

(a) A person commits the offense of computer tampering when he knowingly and without the authorization of a computer's owner, as defined in Section 15-2 of this Code, or in excess of the authority granted to him:

(1) Accesses or causes to be accessed a computer or

any part thereof, or a program or data;

(2) Accesses or causes to be accessed a computer or

any part thereof, or a program or data, and obtains data or services;

(3) Accesses or causes to be accessed a computer or

any part thereof, or a program or data, and damages or destroys the computer or alters, deletes or removes a computer program or data;

(4) Inserts or attempts to insert a "program" into a

computer or computer program knowing or having reason to believe that such "program" contains information or commands that will or may damage or destroy that computer, or any other computer subsequently accessing or being accessed by that computer, or that will or may alter, delete or remove a computer program or data from that computer, or any other computer program or data in a computer subsequently accessing or being accessed by that computer, or that will or may cause loss to the users of that computer or the users of a computer which accesses or which is accessed by such "program";

(5) Falsifies or forges electronic mail transmission

information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers;

(a-5) It shall be unlawful for any person knowingly to sell, give, or otherwise distribute or possess with the intent to sell, give, or distribute software which (1) is primarily designed or produced for the purpose of facilitating or enabling the falsification of electronic

mail transmission information or other routing information; (2) has only a limited commercially significant purpose or use other than to facilitate or enable the falsification of electronic mail transmission information or other routing information; or (3) is marketed by that person or another acting in concert with that person with that person's knowledge for use in facilitating or enabling the falsification of electronic mail transmission information or other routing information.

(b) Sentence.

(1) A person who commits the offense of computer

tampering as set forth in subsection (a) (1), (a) (5), or (a-5) of this Section shall be guilty of a Class B misdemeanor.

(2) A person who commits the offense of computer

tampering as set forth in subsection (a) (2) of this Section shall be guilty of a Class A misdemeanor and a Class 4 felony for the second or subsequent offense.

(3) A person who commits the offense of computer

tampering as set forth in subsection (a) (3) or subsection (a) (4) of this Section shall be guilty of a Class 4 felony and a Class 3 felony for the second or subsequent offense.

(4) If the injury arises from the transmission of

unsolicited bulk electronic mail, the injured person, other than an electronic mail service provider, may also recover attorney's fees and costs, and may elect, in lieu of actual damages, to recover the lesser of \$10 for each and every unsolicited bulk electronic mail message transmitted in violation of this Section, or \$25,000 per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network.

(5) If the injury arises from the transmission of

unsolicited bulk electronic mail, an injured electronic mail service provider may also recover attorney's fees and costs, and may elect, in lieu of actual damages, to recover the greater of \$10 for each and every unsolicited electronic mail advertisement transmitted in violation of this Section, or \$25,000 per day.

(6) The provisions of this Section shall not be

construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law.

(c) Whoever suffers loss by reason of a violation of subsection (a) (4) of this Section may, in a civil action against the violator, obtain appropriate relief. In a civil action under this Section, the court may award to the prevailing party reasonable attorney's fees and other litigation expenses.

(Source: P.A. 91-233, eff. 1-1-00.)

(720 ILCS 5/16D-4) (from Ch. 38, par. 16D-4)

Sec. 16D-4. Aggravated Computer Tampering. (a) A person commits aggravated computer tampering when he commits the offense of computer tampering as set forth in subsection (a)(3) of Section 16D-3 and he knowingly:

- (1) causes disruption of or interference with vital services or operations of State or local government or a public utility; or
- (2) creates a strong probability of death or great bodily harm to one or more individuals.

(b) Sentence. (1) A person who commits the offense of aggravated computer tampering as set forth in subsection (a)(1) of this Section shall be guilty of a Class 3 felony.

(2) A person who commits the offense of aggravated computer tampering as set forth in subsection (a)(2) of this Section shall be guilty of a Class 2 felony.

(Source: P.A. 86-820.)

(720 ILCS 5/16D-5) (from Ch. 38, par. 16D-5)

Sec. 16D-5. Computer Fraud. (a) A person commits the offense of computer fraud when he knowingly:

(1) Accesses or causes to be accessed a computer or any part thereof, or a program or data, for the purpose of devising or executing any scheme, artifice to defraud, or as part of a deception;

(2) Obtains use of, damages, or destroys a computer or any part thereof, or alters, deletes, or removes any program or data contained therein, in connection with any scheme, artifice to defraud, or as part of a deception; or

(3) Accesses or causes to be accessed a computer or any part thereof, or a program or data, and obtains money or control over any such money, property, or services of another in connection with any scheme, artifice to defraud, or as part of a deception.

(b) Sentence. (1) A person who commits the offense of computer fraud as set forth in subsection (a)(1) of this Section shall be guilty of a Class 4 felony.

(2) A person who commits the offense of computer fraud as set forth in subsection (a)(2) of this Section shall be guilty of a Class 3 felony.

(3) A person who commits the offense of computer fraud as set forth in subsection (a)(3) of this Section shall:

(i) be guilty of a Class 4 felony if the value of the money, property or services is \$1,000 or less; or

(ii) be guilty of a Class 3 felony if the value of the money, property or services is more than \$1,000 but less than \$50,000; or

(iii) be guilty of a Class 2 felony if the value of the money, property or services is \$50,000 or more.

(Source: P.A. 85-926.)

(720 ILCS 5/16D-6) (from Ch. 38, par. 16D-6)

Sec. 16D-6. Forfeiture. 1. Any person who commits the offense of computer fraud as set forth in Section 16D-5 shall forfeit, according to the provisions of this Section, any monies, profits or proceeds, and any interest or property which the sentencing court determines he has acquired or maintained, directly or indirectly, in whole or in part, as a result of such offense. Such person shall also forfeit any interest in, security, claim against, or contractual right of any kind which affords him a source of influence over any enterprise which he has established, operated, controlled, conducted or participated in conducting, where his relationship to or connection with any such thing or activity directly or indirectly, in whole or in part, is traceable to any item or benefit which he has obtained or acquired through computer fraud.

Proceedings instituted pursuant to this Section shall be subject to and conducted in accordance with the following procedures:

(a) The sentencing court shall, upon petition by the prosecuting agency, whether it is the Attorney General or a State's Attorney, at any time following sentencing, conduct a hearing to determine whether any property or property interest is subject to forfeiture under this Section. At the forfeiture hearing the People of the State of Illinois shall have the burden of establishing, by a preponderance of the evidence, that the property or property interests are subject to such forfeiture.

(b) In any action brought by the People of the State of Illinois under this Section, the circuit courts of Illinois shall have jurisdiction to enter such restraining orders, injunctions or prohibitions, or to take such other action in connection with any real, personal, or mixed property or other interest subject to forfeiture, as they shall consider proper.

(c) In any action brought by the People of the State of Illinois under this Section, wherein any restraining order, injunction or prohibition or any other action in connection with any property or interest subject to forfeiture under this Section is sought, the circuit court presiding over the trial of the person or persons charged with computer fraud shall first determine whether there is probable cause to believe that the person or persons so charged have committed the offense of computer fraud and whether the property or interest is subject to forfeiture pursuant to this Section. In order to make this determination, prior to entering any such order, the court shall conduct a hearing without a jury, where the People shall establish: (1) probable cause that the person or persons so charged have committed the offense of computer fraud, and (2) probable cause that any property or interest may be subject to forfeiture pursuant to this Section. Such hearing may be conducted simultaneously with a preliminary hearing if the prosecution is commenced by information or complaint, or by motion of the People at any stage in the proceedings. The court may enter a finding of probable cause at a preliminary hearing following the filing of an information charging the offense of computer fraud or the return of an indictment by a grand jury charging the offense of computer fraud as sufficient evidence of probable cause for purposes of this Section. Upon such a finding, the circuit court shall enter such restraining order, injunction or prohibition, or shall take such other action in connection with any such property or other interest subject to forfeiture under this Section as is necessary to insure that such property is not removed from the jurisdiction of the court, concealed, destroyed or otherwise disposed of by the owner or holder of that

property or interest prior to a forfeiture hearing under this Section. The Attorney General or State's Attorney shall file a certified copy of such restraining order, injunction or other prohibition with the recorder of deeds or registrar of titles of each county where any such property of the defendant may be located. No such injunction, restraining order or other prohibition shall affect the rights of any bona fide purchaser, mortgagee, judgment creditor or other lienholder arising prior to the date of such filing. The court may, at any time, upon verified petition by the defendant, conduct a hearing to release all or portions of any such property or interest which the court previously determined to be subject to forfeiture or subject to any restraining order, injunction, prohibition or other action. The court may release such property to the defendant for good cause shown and within the sound discretion of the court.

(d) Upon conviction of a person under Section 16D-5, the court shall authorize the Attorney General to seize and sell all property or other interest declared forfeited under this Act, unless such property is required by law to be destroyed or is harmful to the public. The court may order the Attorney General to segregate funds from the proceeds of such sale sufficient: (1) to satisfy any order of restitution, as the court may deem appropriate; (2) to satisfy any legal right, title, or interest which the court deems superior to any right, title, or interest of the defendant at the time of the commission of the acts which gave rise to forfeiture under this Section; or (3) to satisfy any bona-fide purchaser for value of the right, title, or interest in the property who was without reasonable notice that the property was subject to forfeiture. Following the entry of an order of forfeiture, the Attorney General shall publish notice of the order and his intent to dispose of the property. Within the 30 days following such publication, any person may petition the court to adjudicate the validity of his alleged interest in the property.

After the deduction of all requisite expenses of administration and sale, the Attorney General shall distribute the proceeds of such sale, along with any moneys forfeited or seized as follows:

(1) 50% shall be distributed to the unit of local government whose officers or employees conducted the investigation into computer fraud and caused the arrest or arrests and prosecution leading to the forfeiture. Amounts distributed to units of local government shall be used for training or enforcement purposes relating to detection, investigation or prosecution of financial crimes, including computer fraud. In the event, however, that the investigation, arrest or arrests and prosecution leading to the forfeiture were undertaken solely by a State agency, the portion provided hereunder shall be paid into the State Police Services Fund of the Illinois Department of State Police to be used for training or enforcement purposes relating to detection, investigation or prosecution of financial crimes, including computer fraud.

(2) 50% shall be distributed to the county in which the prosecution and petition for forfeiture resulting in the forfeiture was instituted by the State's Attorney, and deposited in a special fund in the county treasury and appropriated to the State's Attorney for use in training or enforcement purposes relating to detection, investigation or prosecution of financial crimes, including computer fraud. Where a prosecution and petition for forfeiture resulting in the forfeiture has been maintained by the Attorney General, 50% of the proceeds shall be paid into the Attorney General's Financial Crime Prevention Fund. Where the Attorney General and the State's Attorney have participated jointly

in any part of the proceedings, 25% of the proceeds forfeited shall be paid to the county in which the prosecution and petition for forfeiture resulting in the forfeiture occurred, and 25% shall be paid to the Attorney General's Financial Crime Prevention Fund to be used for the purposes as stated in this subsection.

2. Where any person commits a felony under any provision of this Code or another statute and the instrumentality used in the commission of the offense, or in connection with or in furtherance of a scheme or design to commit the offense, is a computer owned by the defendant or if the defendant is a minor, owned by his or her parents or legal guardian, the computer shall be subject to the provisions of this Section. However, in no case shall a computer, or any part thereof, be subject to the provisions of the Section if the computer accessed in the commission of the offense is owned or leased by the victim or an innocent third party at the time of the commission of the offense or if the rights of creditors, lienholders, or any person having a security interest in the computer at the time of the commission of the offense shall be adversely affected.

(Source: P.A. 85-1042.)

(720 ILCS 5/16D-7) (from Ch. 38, par. 16D-7)

Sec. 16D-7. Rebuttable Presumption - without authority. In the event that a person accesses or causes to be accessed a computer, which access requires a confidential or proprietary code which has not been issued to or authorized for use by that person, a rebuttable presumption exists that the computer was accessed without the authorization of its owner or in excess of the authority granted.

(Source: P.A. 85-926.)