

CYBERCRIME LAWS OF THE UNITED STATES

Statutes related to fraud, intrusion, identity theft, damage to systems, or on-line gambling

18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information

18 U.S.C. § 1028A – Aggravated identity theft

18 U.S.C. § 1029 – Fraud and related activity in connection with access devices

18 U.S.C. § 1030 – Fraud and related activity in connection with computers

18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail

18 U.S.C. § 1343 – Fraud by wire, radio, or television

18 U.S.C. § 1362 – [Malicious mischief related to] Communications lines, stations, or systems

The Unlawful Internet Gambling Enforcement Act of 2006

18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information

- (a) Whoever, in a circumstance described in subsection (c) of this section—
- (1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;
 - (2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;
 - (3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;
 - (4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;
 - (5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;
 - (6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;
 - (7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or
 - (8) knowingly traffics in false authentication features for use in false identification documents, document-making implements, or means of identification;
- shall be punished as provided in subsection (b) of this section.
- (b) The punishment for an offense under subsection (a) of this section is—
- (1) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is—
 - (A) the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be—
 - (i) an identification document or authentication feature issued by or under the authority of the United States; or
 - (ii) a birth certificate, or a driver's license or personal identification card;
 - (B) the production or transfer of more than five identification documents, authentication features, or false identification documents;
 - (C) an offense under paragraph (5) of such subsection; or
 - (D) an offense under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating \$1,000 or more during any 1-year period;
 - (2) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 5 years, or both, if the offense is—
 - (A) any other production, transfer, or use of a means of identification, an identification document, authentication feature, or a false identification document; or
 - (B) an offense under paragraph (3) or (7) of such subsection;

- (3) a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed—
- (A) to facilitate a drug trafficking crime (as defined in section 929 (a)(2));
 - (B) in connection with a crime of violence (as defined in section 924 (c)(3)); or
 - (C) after a prior conviction under this section becomes final;
- (4) a fine under this title or imprisonment for not more than 30 years, or both, if the offense is committed to facilitate an act of domestic terrorism (as defined under section 2331 (5) of this title) or an act of international terrorism (as defined in section 2331 (1) of this title);
- (5) in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and
- (6) a fine under this title or imprisonment for not more than one year, or both, in any other case.
- (c) The circumstance referred to in subsection (a) of this section is that—
- (1) the identification document, authentication feature, or false identification document is or appears to be issued by or under the authority of the United States or the document-making implement is designed or suited for making such an identification document, authentication feature, or false identification document;
 - (2) the offense is an offense under subsection (a)(4) of this section; or
 - (3) either—
 - (A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or
 - (B) the means of identification, identification document, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.
- (d) In this section and section 1028A—
- (1) the term “authentication feature” means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;
 - (2) the term “document-making implement” means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;
 - (3) the term “identification document” means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;
 - (4) the term “false identification document” means a document of a type intended or commonly accepted for the purposes of identification of individuals that—
 - (A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and
 - (B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;
 - (5) the term “false authentication feature” means an authentication feature that—
 - (A) is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit;

(B) is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document, document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or

(C) appears to be genuine, but is not;

(6) the term “issuing authority”—

(A) means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and

(B) includes the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization;

(7) the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029 (e));

(8) the term “personal identification card” means an identification document issued by a State or local government solely for the purpose of identification;

(9) the term “produce” includes alter, authenticate, or assemble;

(10) the term “transfer” includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others;

(11) the term “State” includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States; and

(12) the term “traffic” means—

(A) to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value; or

(B) to make or obtain control of with intent to so transport, transfer, or otherwise dispose of.

(e) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title.

(f) Attempt and Conspiracy.— Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

(g) Forfeiture Procedures.— The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(h) Forfeiture; Disposition.— In the circumstance in which any person is convicted of a violation of subsection (a), the court shall order, in addition to the penalty prescribed, the forfeiture and destruction or

other disposition of all illicit authentication features, identification documents, document-making implements, or means of identification.

(i) Rule of Construction.— For purpose of subsection (a)(7), a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification.

18 U.S.C. § 1028A – Aggravated identity theft

(a) Offenses.—

(1) In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2) Terrorism offense.— Whoever, during and in relation to any felony violation enumerated in section 2332b (g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

(b) Consecutive Sentence.— Notwithstanding any other provision of law—

(1) a court shall not place on probation any person convicted of a violation of this section;

(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used;

(3) in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the Sentencing Commission pursuant to section 994 of title 28.

(c) Definition.— For purposes of this section, the term “felony violation enumerated in subsection (c)” means any offense that is a felony violation of—

(1) section 641 (relating to theft of public money, property, or rewards), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans);

(2) section 911 (relating to false personation of citizenship);

(3) section 922 (a)(6) (relating to false statements in connection with the acquisition of a firearm);

(4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028 (a)(7);

(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud);

(6) any provision contained in chapter 69 (relating to nationality and citizenship);

(7) any provision contained in chapter 75 (relating to passports and visas);

(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6823) (relating to obtaining customer information by false pretenses);

(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card);

(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or

(11) section 208, 811, 1107(b), 1128B(a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307 (b), 1320a–7b (a), and 1383a) (relating to false statements relating to programs under the Act).

18 U.S.C. § 1029 – Fraud and related activity in connection with access devices

(a) Whoever—

- (1)** knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
- (2)** knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;
- (3)** knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
- (4)** knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;
- (5)** knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000;
- (6)** without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—
 - (A)** offering an access device; or
 - (B)** selling information regarding or an application to obtain an access device;
- (7)** knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;
- (8)** knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;
- (9)** knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or
- (10)** without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

- (1)** Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.
- (2)** Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) Penalties.—

- (1) Generally.—** The punishment for an offense under subsection (a) of this section is—
 - (A)** in the case of an offense that does not occur after a conviction for another offense under this section—
 - (i)** if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

(2) Forfeiture procedure.— The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term “access device” means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) the term “counterfeit access device” means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) the term “unauthorized access device” means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4) the term “produce” includes design, alter, authenticate, duplicate, or assemble;

(5) the term “traffic” means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(6) the term “device-making equipment” means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;

(7) the term “credit card system member” means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;

(8) the term “scanning receiver” means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument;

(9) the term “telecommunications service” has the meaning given such term in section 3 of title I of the Communications Act of 1934 (47 U.S.C. 153);

(10) the term “facilities-based carrier” means an entity that owns communications transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communications Commission under the authority of title III of the Communications Act of 1934; and

(11) the term “telecommunication identifying information” means electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title. For

purposes of this subsection, the term “State” includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(g)

(1) It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that subsection for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining telecommunications service provided by another facilities-based carrier without the authorization of such carrier.

(2) In a prosecution for a violation of subsection (a)(9), (other than a violation consisting of producing or trafficking) it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) that the conduct charged was engaged in for research or development in connection with a lawful purpose.

(h) Any person who, outside the jurisdiction of the United States, engages in any act that, if committed within the jurisdiction of the United States, would constitute an offense under subsection (a) or (b) of this section, shall be subject to the fines, penalties, imprisonment, and forfeiture provided in this title if—

(1) the offense involves an access device issued, owned, managed, or controlled by a financial institution, account issuer, credit card system member, or other entity within the jurisdiction of the United States; and

(2) the person transports, delivers, conveys, transfers to or through, or otherwise stores, secrets, or holds within the jurisdiction of the United States, any article used to assist in the commission of the offense or the proceeds of such offense or property derived therefrom.

18 U.S.C. § 1030 – Fraud and related activity in connection with computers**(a) Whoever—**

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)

(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

- (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
- (6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—
 - (A) such trafficking affects interstate or foreign commerce; or
 - (B) such computer is used by or for the Government of the United States;
- (7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

- (1)
 - (A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
 - (B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (2)
 - (A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
 - (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—
 - (i) the offense was committed for purposes of commercial advantage or private financial gain;
 - (ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
 - (iii) the value of the information obtained exceeds \$5,000; and
 - (C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (3)
 - (A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
 - (B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
- (4)

- (A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;
- (B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
- (C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
- (5)
- (A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
- (B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.
- (d)
- (1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
- (2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056 (a) of this title.
- (3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
- (e) As used in this section—
- (1) the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
- (2) the term “protected computer” means a computer—
- (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
- (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
- (3) the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
- (4) the term “financial institution” means—
- (A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;
- (B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
- (C) a credit union with accounts insured by the National Credit Union Administration;
- (D) a member of the Federal home loan bank system and any home loan bank;

- (E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
 - (F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
 - (G) the Securities Investor Protection Corporation;
 - (H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
 - (I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;
- (5) the term “financial record” means information derived from any record held by a financial institution pertaining to a customer’s relationship with the financial institution;
- (6) the term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
- (7) the term “department of the United States” means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
- (8) the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information;
- (9) the term “government entity” includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
- (10) the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
- (11) the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
- (12) the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
- (f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
- (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.
- (h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

18 U.S.C. § 1037 – Fraud and related activity in connection with electronic mail

- (a) In General.**— Whoever, in or affecting interstate or foreign commerce, knowingly—
- (1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,
 - (2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,
 - (3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,
 - (4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or
 - (5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,
- or conspires to do so, shall be punished as provided in subsection (b).
- (b) Penalties.**— The punishment for an offense under subsection (a) is—
- (1) a fine under this title, imprisonment for not more than 5 years, or both, if—
 - (A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or
 - (B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;
 - (2) a fine under this title, imprisonment for not more than 3 years, or both, if—
 - (A) the offense is an offense under subsection (a)(1);
 - (B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;
 - (C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period;
 - (D) the offense caused loss to one or more persons aggregating \$5,000 or more in value during any 1-year period;
 - (E) as a result of the offense any individual committing the offense obtained anything of value aggregating \$5,000 or more during any 1-year period; or
 - (F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and
 - (3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.
- (c) Forfeiture.**—
- (1) **In general.**— The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States—
 - (A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and
 - (B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

(2) Procedures.— The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all stages of a criminal forfeiture proceeding under this section.

(d) Definitions.— In this section:

(1) Loss.— The term “loss” has the meaning given that term in section 1030 (e) of this title.

(2) Materially.— For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

(3) Multiple.— The term “multiple” means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

(4) Other terms.— Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.”.

18 U.S.C. § 1343 – Fraud by wire, radio, or television

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.

18 U.S.C. § 1362 – [Malicious mischief related to] Communications lines, stations, or systems

Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States.

The Unlawful Internet Gambling Enforcement Act of 2006

Came into effect on October 13, 2006, and amends United States Code, Title 53, Chapter 31

THIS IS A SUMMARY OF THE ACT, PREPARED BY THE U.S. CONGRESSIONAL RESEARCH SERVICE:

Title I: Modernization of the Wire Act of 1961 –

(Sec. 101) Amends the federal criminal code to expand the definition of "wire communication facility" (renamed "communication facility") to include fixed or mobile (i.e., wireless) communication facilities.

Defines "bets and wagers" to include bets for contests, sporting events, games predominantly subject to chance, and lotteries. Excludes from such definition: (1) activities governed by securities laws; (2) transactions under the Commodity Exchange Act; (3) over-the-counter derivative instruments; (4) contracts of indemnity or guarantee; (4) contracts for life, health, or accident insurance; and (5) reward programs or contests conducted by businesses.

(Sec. 102) Modifies existing prohibitions against interstate gambling to prohibit the use of a communication facility to transmit: (1) bets or wagers; (2) information assisting in the placing of bets or wagers; or (3) a communication which entitles the recipient to receive money or credit as a result of bets or wagers or for information assisting in the placing of bets or wagers.

Prohibits any individual from accepting, in connection with the placing of bets or wagers to or from the United States: (1) credit, or the proceeds of credit; (2) electronic funds transfers; (3) checks, drafts, or similar instruments; or (4) the proceeds of any other form of financial transaction as prescribed by Treasury regulations.

Imposes a fine and/or prison term of up to five years for violations.

Requires any common carrier which receives notice of a violation of this Act by one of its communication facilities to discontinue or refuse service to such facility. Grants such common carrier immunity from liability for discontinuing or refusing such service.

(Sec. 103) Grants U.S. district courts original and exclusive jurisdiction to prevent and restrain violations of the Internet gambling ban. Authorizes the Attorney General or any state attorney general to institute proceeding to enforce an Internet gambling ban.

(Sec. 104) Authorizes appropriations to the Department of Justice in FY2007-FY2010 for investigations and prosecutions of unlawful Internet gambling.

(Sec. 105) Declares that nothing in this Act may be construed to prohibit any activity allowed under the Interstate Horseracing Act or to preempt any state law prohibiting gambling.

(Sec. 106) Expresses the sense of Congress that this Act does not address the legality of certain horse racing activities under federal law.

Title II: Policies and Procedures Required to Prevent Payments for Unlawful Gambling - Amends the federal criminal code to prohibit persons engaged in a gambling business from knowingly accepting credit, electronic fund transfers, checks, drafts, or similar financial instruments or the proceeds of any

other financial transaction in connection with unlawful Internet gambling (this prohibition is defined by this Act as a "restricted transaction").

Directs the Secretary of the Treasury and the Board of Governors of the Federal Reserve System to prescribe regulations to identify and block restricted transactions. Grants immunity from civil liability for blocking a restricted transaction or one which is reasonably believed to be a restricted transaction.

Title III: Internet Gambling in or through Foreign Jurisdictions - Calls upon the U.S. government, in deliberations with foreign governments, to: (1) encourage cooperation by foreign governments in identifying whether Internet gambling operations are being used for money laundering, corruption, or other crimes; (2) advance policies that promote international cooperation in enforcing this Act; and (3) encourage the Financial Action Task Force on Money Laundering to study the extent to which Internet gambling operations are being used for money laundering purposes.

Directs the Secretary of the Treasury to report to Congress annually on deliberations between the United States and other countries on Internet gambling.