

Effective: September 26, 2008

United States Code Annotated Currentness

Title 18. Crimes and Criminal Procedure (Refs & Annos)

▣ Part I. Crimes (Refs & Annos)

▣ Chapter 47. Fraud and False Statements (Refs & Annos)

→ **§ 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;

(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) 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;

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

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(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; [FN1]

(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--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

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

(b) Whoever conspires to commit or 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), 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) 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 subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense 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;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subsection (a) (5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for--

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

[(5) Repealed. Pub.L. 110-326, Title II, § 204(a)(2)(D), Sept. 26, 2008, 122 Stat. 3562]

(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 or affecting 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, [FN2] 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 accessor 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 subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(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).

(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section [FN3]

CREDIT(S)

(Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190, and amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub.L. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub.L. 103-322, Title XXIX, § 290001(b) to (f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub.L. 107-56, Title V, § 506(a), Title VIII, § 814, Oct. 26, 2001, 115 Stat. 366, 382; Pub.L. 107-273, Title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub.L. 107-296, Title II, § 225(g), Nov. 25, 2002, 116 Stat. 2158; Pub.L. 110-326, Title II, §§ 203, 204(a), 205 to 208, Sept. 26, 2008, 122 Stat. 3561, 3563.)

[FN1] So in original. Probably should be followed by "or".

[FN2] So in original. The comma probably should not appear.

[FN3] So in original. A period probably should appear.

HISTORICAL AND STATUTORY NOTES

Revision Notes and Legislative Reports

1984 Acts. House Report No. 98-1030 and House Conference Report No. 98-1159, see 1984 U.S. Code Cong. and Adm. News, p. 3182.

1986 Acts. House Report No. 99-797, see 1986 U.S. Code Cong. and Adm. News, p. 6138.

1989 Acts. House Report No. 101-54(Parts I to VII) and House Conference Report No. 101-222, see 1989 Code Cong. and Adm. News, p. 86.

1990 Acts. House Report Nos. 101-681(Parts I and II), 101-736, Senate Report No. 101-460, and Statement by President, see 1990 U.S. Code Cong. and Adm. News, p. 6472.

1994 Acts. House Report Nos. 103-324, 103-489, and House Conference Report No. 103-711, see 1994 U.S. Code Cong. and Adm. News, p. 1801.

1996 Acts. House Report No. 104-788, see 1996 U.S. Code Cong. and Adm. News, p. 4021.

2002 Acts. House Conference Report No. 107-685 and Statement by President, see 2002 U.S. Code Cong. and Adm. News, p. 1120.

House Report No. 107-609(Part I) and Statement by President, see 2002 U.S. Code Cong. and Adm. News, p. 1352.

2008 Acts. House Report No. 110-696, see 2008 U.S. Code Cong. and Adm. News, p. 1328.

References in Text

The Federal Reserve Act, referred to in text, is Act Dec. 23, 1913, c. 6, 38 Stat. 251, as amended, which is classified principally to chapter 3 of Title 12, 12 U.S.C.A. § 221 et seq. Section 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I of chapter 6 of Title 12, 12 U.S.C.A. § 601 et seq. Section 25(a) of the Federal Reserve Act, which is classified to subchapter II of chapter 6 of Title 12, 12 U.S.C.A. § 611 et seq., was renumbered section 25A by Pub.L. 102-242, Title I, § 142(e)(2), Dec. 10, 1991, 105 Stat. 2281. See Tables and 12 U.S.C.A. § 226 for complete classification.

Reference to “paragraph y of section 11 of the Atomic Energy Act of 1954”, referred to in subsec. (a)(1) is classified to section 2014(y) of Title 42, Public Health and Welfare.

The Fair Credit Reporting Act, referred to in subsec. (a)(2)(A), is Title VI of Pub.L. 90-321 as added by Pub.L. 91-508, Title VI, Oct. 26, 1970, 84 Stat. 1127, which is classified to subchapter III (section 1681 et seq.) of chapter 41 of Title 15, Commerce and Trade.

Section 11y of the Atomic Energy Act of 1954, referred to in subsec. (d)(2), is Aug. 1, 1946, c. 724, Title I, § 11(y), as added Aug. 30, 1954, c. 1073, § 1, 68 Stat. 922, as amended, which is classified to 42 U.S.C.A. § 2014(y).

The Farm Credit Act of 1971, referred to in subsec. (e)(4)(E), is Pub.L. 92-181, Dec. 10, 1971, 85 Stat. 585, as amended, which is classified generally to chapter 23 (section 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

Section 15 of the Securities Exchange Act of 1934, referred to in subsec. (e)(4)(F), is classified to section 78o of Title 15, Commerce and Trade.

Section 1(b) of the International Banking Act of 1978, referred to in subsec. (e)(4)(H), is classified to section 3101 of Title 12, Banks and Banking.

The date of the enactment of this subsection, referred to in subsec. (h), means the date of the enactment of Pub.L. 103-322, 108 Stat. 1796, which enacted subsec. (h) and was approved Sept. 13, 1994.

Amendments

2008 Amendments. Subsec. (a)(2)(C). Pub.L. 110-326, § 203, struck out “if the conduct involved an interstate or foreign communication” following “protected computer”.

Subsec. (a)(5). Pub.L. 110-326, § 204(a)(1), rewrote par. (5), which formerly read:

“(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;”.

Subsec. (a)(7). Pub.L. 110-326, § 205, rewrote par. (7), which formerly read: “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;”.

Subsec. (b). Pub.L. 110-326, § 206, inserted “conspires to commit or” after “Whoever”.

Subsec. (c)(2)(A). Pub.L. 110-326, § 204(a)(2)(A), struck out “(a)(5)(A)(iii),” preceding “or (a)(6) of this section”.

Subsec. (c)(3)(B). Pub.L. 110-326, § 204(a)(2)(B), struck out “(a)(5)(A)(iii),” preceding “or (a)(7) of this section”.

Subsec. (c)(4). Pub.L. 110-326, § 204(a)(2)(C), rewrote par. (4), which formerly read:

“(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”.

Subsec. (c)(5). Pub.L. 110-326, § 204(a)(2)(D), struck out par. (5), which formerly read:

“(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.”

Subsec. (e)(2)(B). Pub.L. 110-326, § 207, inserted “or affecting” after “which is used in”.

Subsec. (g). Pub.L. 110-326, § 204(a)(3), in the second sentence, struck out “in clauses (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B)” and inserted “in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)”; in the third sentence, struck out “subsection (a)(5)(B)(i)” and inserted “subsection (c)(4)(A)(i)(I)”.

Subsecs. (i), (j). Pub.L. 110-326, § 208, added subsecs. (i) and (j).

2002 Amendments. Subsec. (a)(5)(B). Pub.L. 107-273, § 4005(a)(3), made technical amendments requiring no change in text.

Subsec. (c)(2)(B). Pub.L. 107-273, § 4002(b)(1), made technical amendments requiring no change in text.

Subsec. (c)(2)(B)(iii). Pub.L. 107-273, § 4002(b)(12)(A), inserted “and” at the end.

Subsec. (c)(3)(B). Pub.L. 107-273, § 4002(d)(3), inserted a comma after “(a)(4)” but required no change in text.

Pub.L. 107-296, § 225(g)(1), struck out “and” at the end.

Subsec. (c)(4)(A). Pub.L. 107-296, § 225(g)(2), inserted “except as provided in paragraph (5),” preceding “a fine under this title”.

Subsec. (c)(4)(C). Pub.L. 107-296, § 225(g)(2), (3), inserted “except as provided in paragraph (5),” preceding “a fine under this title”, and struck out the period at the end and inserted “; and”, respectively.

Subsec. (c)(5). Pub.L. 107-296, § 225(g)(4), added par. (5).

Subsec. (e)(4)(I). Pub.L. 107-273, § 4002(b)(12)(B), inserted a semicolon at the end.

2001 Amendments. Subsec. (a)(5). Pub.L. 107-56, § 814(a), inserted "(i)" after "(A)"; redesignated former subpars. (B) and (C) as clauses (ii) and (iii), respectively; added "and" at the end of clause (iii), as so redesignated; and added par. (B)(i) to (v).

Subsec. (a)(7). Pub.L. 107-56, § 814(b), struck out " , firm, association, educational institution, financial institution, government entity, or other legal entity," after "from any person".

Subsec. (c)(2)(A). Pub.L. 107-56, § 814(c)(1)(A), inserted "except as provided in subparagraph (B)," before "a fine"; substituted "(a)(5)(A)(iii)" for "(a)(5)(C)"; and struck out "and" at the end.

Subsec. (c)(2)(B). Pub.L. 107-56, § 814(c)(1)(B), inserted "or an attempt to commit an offense punishable under this subparagraph," after "subsection (a)(2)," in the matter preceding clause (i).

Subsec. (c)(2)(C). Pub.L. 107-56, § 814(c)(1)(C), struck out "and" at the end.

Subsec. (c)(3)(A). Pub.L. 107-56, § 814(c)(2)(A), struck out " , (a)(5)(A), (a)(5)(B)" after subsection "(a)(4)".

Subsec. (c)(3)(B). Pub.L. 107-56, § 814(c)(2)(A), (B), struck out " , (a)(5)(A), (a)(5)(B)," after "subsection (a)(4)" and substituted "(a)(5)(A)(iii)" for "(a)(5)(C)".

Subsec. (c)(4). Pub.L. 107-56, § 814(c)(3), inserted par. (4).

Subsec. (d). Pub.L. 107-56, § 506(a), rewrote subsec. (d), which formerly read: "The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of 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."

Subsec. (e)(2)(B). Pub.L. 107-56, § 814(d)(1), inserted " , 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" after "foreign commerce or communication".

Subsec. (e)(7). Pub.L. 107-56, § 814(d)(2), struck out "and" at the end.

Subsec. (e)(8). Pub.L. 107-56, § 814(d)(3), rewrote par. (8), which formerly read:

“(8) the term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information, that--

“(A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals;

“(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

“(C) causes physical injury to any person; or

“(D) threatens public health or safety; and”.

Subsec. (e)(9). Pub.L. 107-56, § 814(d)(4), substituted a semicolon for the period.

Subsec. (e)(10) to (12). Pub.L. 107-56, § 814(d)(5), inserted pars. (10) to (12).

Subsec. (g). Pub.L. 107-56, § 814(e), substituted “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.” for “Damages for violations involving damage as defined in subsection (e)(8)(A) are limited to economic damages.” and inserted “No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.”

1996 Amendments. Subsec. (a)(1). Pub.L. 104-294, § 201(1)(A), amended par. (1) generally. Prior to amendment, par. (1) read as follows: “knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains 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 the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation;”.

Subsec. (a)(2)(A) to (C). Pub.L. 104-294, § 201(1)(B), added subpars. (B) and (C), and designated existing provisions relating to obtaining information contained in financial institution records, or of a card issuer, or contained in a file of a consumer reporting agency on a consumer, as subpar. (A).

Subsec. (a)(3). Pub.L. 104-294, § 201(1)(C), substituted “any nonpublic computer of a department or agency” for “any computer of a department or agency” and “such conduct affects that use by or for the Government of the United States” for “such conduct adversely affects the use of the Government's operation of such computer”.

Subsec. (a)(4). Pub.L. 104-294, § 201(1)(D), substituted “accesses a protected computer” for “accesses a Federal interest computer” and inserted, before the semicolon, “and the value of such use is not more than \$5,000 in any 1-year period”.

Subsec. (a)(5). Pub.L. 104-294, § 201(1)(E), amended par. (5) generally, substituting provisions relating to one who knowingly causes the transmission of a program, information, code, or command, and intentionally causes damage without authorization to a protected computer, or intentionally accesses a protected computer without authorization and recklessly or otherwise causes damage, for provisions relating to one who through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to such computer or systems with the intent to cause damage to or deny usage of such computer or systems, or knowingly and with reckless disregard of a substantial and unjustifiable risk that such transmission will cause damage to or deny usage of such computer or systems, and does cause such damage or denial of usage and such transmission occurs without authorization and causes loss of more than \$1,000 to, or impairs medical care of, one or more individuals.

Subsec. (a)(5)(B)(ii)(II)(bb). Pub.L. 104-294, § 604(b)(36)(A), inserted “or” at the end thereof.

Subsec. (a)(7). Pub.L. 104-294, § 201(1)(G), added par. (7).

Subsec. (c)(1). Pub.L. 104-294, § 201(2)(A), substituted “this section” for “such subsection” wherever appearing.

Subsec. (c)(1)(B). Pub.L. 104-294, § 604(b)(36)(B), struck out “and” which followed the semicolon at the end thereof.

Subsec. (c)(2)(A). Pub.L. 104-294, § 201(2)(B)(i), inserted “, (a)(5)(C),” following “(a)(3)” and substituted “this section” for “such subsection”.

Subsec. (c)(2)(B). Pub.L. 104-294, § 201(2)(B)(iii), added subpar. (B). Former subpar. (B) redesignated (C).

Subsec. (c)(2)(C). Pub.L. 104-294, § 201(2)(B)(ii), (iv), redesignated former subpar. (B) as (C), substituted “this section” for “such subsection”, and inserted “and” at the end thereof.

Subsec. (c)(3)(A). Pub.L. 104-294, § 201(2)(C)(i), substituted “(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)” for “(a)(4) or (a)(5)(A)” and “this section” for “such subsection”.

Subsec. (c)(3)(B). Pub.L. 104-294, § 201(2)(C)(ii), substituted “(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)” for “(a)(4) or (a)(5)(A)” and “this section” for “such subsection”.

Subsec. (c)(4). Pub.L. 104-294, § 201(2)(D), struck out par. (4) which read as follows: “(4) a fine under this title or imprisonment for not more than 1 year, or both, in the case of an offense under subsection (a)(5)(B).”

Subsec. (d). Pub.L. 104-294, § 201(3), inserted “subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6)

of” preceding “this section.”.

Subsec. (e)(2). Pub.L. 104-294, § 201(4)(A)(i), substituted “protected computer” for “Federal interest computer”.

Subsec. (e)(2)(A). Pub.L. 104-294, § 201(4)(B)(ii), substituted “that use by or for the financial institution or the Government” for “the use of the financial institution's operation or the Government's operation of such computer”.

Subsec. (e)(2)(B). Pub.L. 104-294, § 201(4)(A)(iii), amended subpar. (b) generally. Prior to amendment subpar. (B) read as follows: “(B) which is one of two or more computers used in committing the offense, not all of which are located in the same State;”.

Subsec. (e)(8), (9). Pub.L. 104-294, § 201(4)(B) to (D), added pars. (8) and (9).

Subsec. (g). Pub.L. 104-294, § 604(b)(36)(C), substituted “this section” for “the section”.

Pub.L. 104-294, § 201(5), deleted “, other than a violation of subsection (a)(5)(B),” which followed “by reason of a violation of the section” and substituted “involving damage as defined in subsection (e)(8)(A)” for “of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)”.

Subsec. (h). Pub.L. 104-294, § 604(b)(36)(D), substituted “subsection (a)(5)” for “section 1030(a)(5) of title 18, United States Code”.

1994 Amendments. Subsec. (a)(3). Pub.L. 103-322, § 290001(f), substituted “adversely affects” for “affects”.

Subsec. (a)(5). Pub.L. 103-322, § 290001(b), completely revised par. (5). Prior to revision par. (5) related only to a person who “intentionally accesses a Federal interest computer without authorization, and by means of one or more of such conduct alters, damages, or destroys any information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby causes loss to one or more others of a value aggregating \$1,000 or more during any one year period, or modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals”.

Subsec. (c)(3)(A). Pub.L. 103-322, § 290001(c)(2), substituted “(a)(5)(A) of this section” for “(a)(5) of this section”.

Subsec. (c)(4). Pub.L. 103-322, § 290001(c)(1), (3), (4), added par. (4).

Subsec. (g). Pub.L. 103-322, § 290001(d), added subsec. (g).

Subsec. (h). Pub.L. 103-322, § 290001(e), added subsec. (h).

1990 Amendments. Subsec. (a)(1). Pub.L. 101-647, § 3533, substituted “paragraph y of section 11” for “paragraph r of section 11”.

Subsec. (e)(3). Pub.L. 101-647 inserted “commonwealth,” before “possession or territory of the United States”.

Subsec. (e)(4)(H), (I). Pub.L. 101-647, § 2597(j), added subpars. (H) and (I).

1989 Amendments. Subsec. (e)(4)(A). Pub.L. 101-73, § 962(a)(5)(A), substituted “an institution” for “a bank”.

Subsec. (e)(4)(C) to (H). Pub.L. 101-73, § 962(a)(5)(B), (C), redesignated former subpars. (D) to (H) as (C) to (G), respectively, and struck out former subpar. (C), which had included within the definition of the term “financial institution” institutions with accounts insured by the Federal Savings and Loan Insurance Corporation.

1988 Amendments. Subsec. (a)(2). Pub.L. 100-690 inserted a comma after “financial institution” and substituted “title 15,” for “title 15,.”

1986 Amendments. Subsec. (a)(1). Pub.L. 99-474, § 2(c), substituted “or exceeds authorized access” for “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend”.

Subsec. (a)(2). Pub.L. 99-474, § 2(a)(1)-(4), substituted “intentionally” for “knowingly”; struck out “as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.),” following “financial institution,;” struck out “or” appearing at end of par. (2); and added following “financial institution” the phrase “or of a card issuer as defined in section 1602(n) of title 15,.”

Pub.L. 99-474, § 2(c), substituted “or exceeds authorized access” for “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend”.

Subsec. (a)(3). Pub.L. 99-474, § 2(b)(1), added par. (3) and struck out former par. (3) provision which read [Whoever--] “knowingly access a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of the United States

and such conduct affects such operation;”, now covered in par. (5).

Subsec. (a)(3) end text. Pub.L. 99-474, § 2(b)(2), struck out following par. (3) sentence reading “It is not an offense under paragraph (2) or (3) of this subsection in the case of a person having accessed a computer with authorization and using the opportunity such access provides for purposes to which such access does not extend, if the using of such opportunity consists only of the use of the computer.”, now covered in subsec. (a)(4).

Subsec. (a)(4)-(6). Pub.L. 99-474, § 2(d), added pars. (4) to (6).

Subsec. (b). Pub.L. 99-474, § 2(e)(1), (2), struck out par. (1) designation and par. (2) provision respecting specific conspiracy offense and prescribing as a fine an amount not greater than the amount provided as the maximum fine for such offense under subsec. (c) or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsec. (c), or both.

Subsec. (c). Pub.L. 99-474, § 2(f)(9), substituted in opening phrase subsec. “(b)” for “(b)(1)”.

Subsec. (c)(1)(A). Pub.L. 99-474, § 2(f)(1), substituted “under this title” for “of not more than the greater of \$10,000 or twice the value obtained by the offense”.

Subsec. (c)(1)(B). Pub.L. 99-474, § 2(f)(2), substituted “under this title” for “of not more than the greater of \$100,000 or twice the value obtained by the offense”.

Subsec. (c)(2)(A). Pub.L. 99-474, § 2(f)(3), (4), inserted reference to subsec. (a)(6) and substituted “under this title” for “of not more than the greater of \$5,000 or twice the value obtained or loss created by the offense”.

Subsec. (c)(2)(B). Pub.L. 99-474, § 2(f)(3), (5)-(7), inserted reference to subsec. (a)(6) and substituted “under this title” for “of not more than the greater of \$10,000 or twice the value obtained or loss created by the offense”, “not more than” for “not than”, and “; and” for the period at end of subpar. (B), respectively.

Subsec. (c)(3). Pub.L. 99-474, § 2(f)(8), added par. (3).

Subsec. (e). Pub.L. 99-474, § 2(g)(1), substituted at end of introductory phrase a one-em dash for the comma.

Subsec. (e)(1). Pub.L. 99-474, § 2(g)(2), (3), aligned so much of the subsec. so that it be cut in two ems and begin as an indented and designated par. (1), and substituted a semicolon for the period at end thereof.

Subsec. (e)(2)-(7). Pub.L. 99-474, § 2(g)(4), added pars. (2) to (7).

Subsec. (f). Pub.L. 99-474, § 2(h), added subsec. (f).

Effective and Applicability Provisions

2002 Acts. Amendment to this section by Pub.L. 107-296 effective 60 days after Nov. 25, 2002, see Pub.L. 107-296, § 4, set out as a note under 6 U.S.C.A. § 101.

1996 Acts. Amendment by section 604 of Pub.L. 104-294 effective Sept. 13, 1994, see section 604(d) of Pub.L. 104-294, set out as a note under section 13 of this title.

Transfer of Functions

For transfer of the functions, personnel, assets, and obligations of the United States Secret Service, including the functions of the Secretary of the Treasury relating thereto, to the Secretary of Homeland Security, and for treatment of related references, see 6 U.S.C.A. §§ 381, 551(d), 552(d) and 557, and the Department of Homeland Security Reorganization Plan of November 25, 2002, as modified, set out as a note under 6 U.S.C.A. § 542.

Severability of Provisions

If any provision of Pub.L. 101-73 or the application thereof to any person or circumstance is held invalid, the remainder of Pub.L. 101-73 and the application of the provision to other persons not similarly situated or to other circumstances not to be affected thereby, see section 1221 of Pub.L. 101-73, set out as a note under section 1811 of Title 12, Banks and Banking.

Report to Congress

Section 2103 of Pub.L. 98-473 provided that: "The Attorney General shall report to the Congress annually, during the first three years following the date of the enactment of this joint resolution [Oct. 12, 1984], concerning prosecutions under the sections of title 18 of the United States Code added by this chapter [this section]."

CROSS REFERENCES

Optional venue for espionage and related offenses on the high seas, see 18 USCA § 3239.

LAW REVIEW COMMENTARIES

Computer crime. Scott Charney & Kent Alexander, 45 Emory L.J. 931 (1996).

Computer Fraud and Abuse Act of 1986: A measured response to a growing problem. Note, 43 Vand.L.Rev. 453 (1990).

Computer Fraud and Abuse Act of 1986: The saga continues. John A. Potter, 10 Corp., Finance & Bus.L. Section J. 243 (1987).

Computer-related crimes. Adam G. Ciongoli, Jennifer A. DeMarrais, and James Wehner, 31 Am.Crim.L.Rev. 425 (1994).

Computer security and privacy: The third wave of property law. Leslie G. Berkowitz, 33-FEB Colo.Law. 57 (2004).

Cybercrime's scope: Interpreting "access" and "authorization" in computer misuse statutes. Orin S. Kerr, 78 N.Y.U. L. Rev. 1596 (2003).

Defending cyberproperty. Patricia L. Bellia, 79 N.Y.U. L. Rev. 2164 (2004).

Embedded alert software: Weapon against piracy or computer abuse? Robert C. Scheinfeld, 216 N.Y.L.J. 1 (Aug. 13, 1996).

Hacking through the Computer Fraud and Abuse Act. 31 U.C. Davis L.Rev. 283 (1997).

Hactivism: Securing the national infrastructure. Mark G. Milone, 58 Bus.Law. 383 (2002).

Mixed metaphors in cyberspace: Property in information and information systems. Jacqueline Lipton, 35 Loy. U. Chi. L.J. 235 (2003).

Regulating internet advertising. Richard Raysman and Peter Brown, 215 N.Y.L.J. 3 (May 14, 1996).


The 1984 Federal Computer Crime Statute: A partial answer to a pervasive problem. Joseph B. Tompkins, Jr. and Linda A. Mar, 6 Computer/L.J. 459 (1986).

Transnational evidence gathering and local prosecution of international cybercrime. Susan W. Brenner and Joseph J. Schwerha IV, XX J.Marshall J. Computer & Info.L. 347 (2002).

What victims of computer crime should know and do. Stephen Fishbein, 210 N.Y.L.J. 1 (Nov. 12, 1993).

LIBRARY REFERENCES

American Digest System

Copyrights and Intellectual Property  109.

Corpus Juris Secundum

CJS Aliens § 635, Interim Measures for Access to and Coordination of Law Enforcement and Other Information.

CJS Aliens § 1116, Sharing by Federal Agencies of Information Relevant to Admissibility.

CJS Aliens § 1244, Sharing by Federal Agencies of Information Relevant to Deportation.

RESEARCH REFERENCES

ALR Library

2006 ALR, Fed. 2nd Series 6, Construction and Application of U.S.S.G. § 2x1.1, Providing Sentencing Guideline for Conspiracy Not Covered by Specific Offense Guideline.

174 ALR, Fed. 101, Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030).

76 ALR, Fed. 46, Discretionary Exercise of Pendent Jurisdiction of Federal Court Over State Claim When Joined With Claim Arising Under Laws, Treaties, or Constitution of United States.

61 ALR, Fed. 603, Propriety, Under Rule 23 of the Federal Rules of Civil Procedure, of Class Action for Violation of Truth in Lending Act (15 U.S.C.A. §§ 1601 et seq.).

92 ALR 5th 15, Expectation of Privacy in Internet Communications.

81 ALR 5th 41, Internet Web Site Activities of Nonresident Person or Corporation as Conferring Personal Jurisdiction Under Long-Arm Statutes and Due Process Clause.

70 ALR 5th 647, Computer Fraud.

75 ALR 4th 1067, What Constitutes a Public Record or Document Within Statute Making Falsification, Forgery, Mutilation, Removal, or Other Misuse Thereof an Offense.

51 ALR 4th 971, Criminal Liability for Theft Of, Interference With, or Unauthorized Use Of, Computer Programs, Files, or Systems.

97 ALR 3rd 96, Instructions Urging Dissenting Jurors in State Criminal Case to Give Due Consideration to Opinion of Majority (Allen Charge)--Modern Cases.

24 ALR 3rd 532, Construction and Application of State Statutes or Rules of Court Predicating in Personam Jurisdiction Over Nonresidents or Foreign Corporations on the Commission of a Tort Within the State.

Encyclopedias

32 Am. Jur. Proof of Facts 3d 1, Computer Malpractice.

41 Am. Jur. Proof of Facts 3d 1, Recovery and Reconstruction of Electronic Mail as Evidence.

59 Am. Jur. Proof of Facts 3d 1, Proof of Personal Jurisdiction in the Internet Age.

67 Am. Jur. Proof of Facts 3d 249, Proof of Liability for Violation of Privacy of Internet User, by Cookies or Other Means.

74 Am. Jur. Proof of Facts 3d 63, Scams and Cons.

81 Am. Jur. Proof of Facts 3d 113, Identity Theft and Other Misuses of Credit and Debit Cards.

14 Am. Jur. Trials 1, Actions for Unfair Competition -- Trade Secrets.

46 Am. Jur. Trials 687, Failure of Performance in Computer Sales and Leases.

70 Am. Jur. Trials 435, The Defense of a Computer Crime Case.

105 Am. Jur. Trials 1, Employer Liability for Employee Misuse of Internet.

Am. Jur. 2d Computers and the Internet § 19, Federal Statutes.

Am. Jur. 2d Computers and the Internet § 84, Computer Fraud and Abuse Act.

Am. Jur. 2d Computers and the Internet § 85, Computer Fraud and Abuse Act--Definition of Terms "Loss" or "Damage"; Matters Included Within Damages.

Am. Jur. 2d Computers and the Internet § 93, Computer Fraud and Abuse Act; Stored Wire and Electronic Communications and Transactional Records Access Act; Electronic Communications Privacy Act.

Am. Jur. 2d Larceny § 60, Computer Programs, Files, or Systems.

Am. Jur. 2d Telecommunications § 198, Computer Crime.

Forms

Federal Procedural Forms § 65:370.50, Complaint--By Internet Service Provider--Against Spammers--Unfair Business Practices--Computer Fraud and Abuse Act [15 U.S.C.A. §§ 1114, 1116, 1117, 1118, 1125(A); 28 U.S.C.A. § 1.

Federal Procedural Forms § 65:370.70, Complaint--For Declaratory, Injunctive, and Monetary Relief for Libel, Tortious Interference, Unfair Competition, Computer Fraud [18 U.S.C.A. § 1030(A)(2), (G); 28 U.S.C.A. §§ 1331, 1332, 1338.

3B West's Federal Forms § 3986, Quashing a Subpoena Duces Tecum.

27A West's Legal Forms § 10:6, Other Legislation and Related Cases.

Am. Jur. Pl. & Pr. Forms Fraud and Deceit § 197.1, Complaint in Federal Court--Violation of Computer Fraud and Abuse Act--Internet User's Fraud in Disrupting Another's Web Site Operations--For Injunctive Relief and Damages.

Am. Jur. Pl. & Pr. Forms Telecommunications § 150, Complaint in Federal Court--By Internet Service Provider--Against Spammers--Unfair Business Practices--Computer Fraud and Abuse Act.

Am. Jur. Pl. & Pr. Forms Telecommunications § 149.8, Complaint, Petition or Declaration--Allegation--By Isp--Against Bulk E-Mail Spammers--For Violation of Federal Anti-Spamming Statute--Accessing Protected Computer Without Autho.

Am. Jur. Pl. & Pr. Forms Telecommunications § 149.9, Complaint, Petition or Declaration--Allegation--By Isp--Against Bulk E-Mail Spammers--For Violation of Federal Anti-Spamming Statute--Impairing Computer Facilities.

Am. Jur. Pl. & Pr. Forms Telecommunications § 149.16, Complaint, Petition or Declaration--Allegation--By Web-Based E-Mail Service--Against Spammers Using Service--Violation of Federal Computer Fraud and Abuse Act--Unauthorized Us.

Am. Jur. Pl. & Pr. Forms Telecommunications § 149.17, Complaint, Petition or Declaration--Allegation--By Web-Based E-Mail Service--Against Spammers Using Service--Violation of Federal Computer Fraud and Abuse Act--Damage to Compu.

Am. Jur. Pl. & Pr. Forms Trademarks and Tradenames § 123, Complaint in Federal District Court--Against Computer Junk E-Mail Company--False Designation of Origin and Description, Service Mark Infringement and Dilution, Violation of Electronic...

Treatises and Practice Aids

Eckstrom's Licensing in Foreign & Domestic Ops. § 8A:23, Economic Espionage Act of 1996.

Employment Practices Manual § 6:29, Electronic Communications--Overview.

Federal Procedure, Lawyers Edition § 22:250, Offenses for Which Interception May be Authorized.

Federal Procedure, Lawyers Edition § 72:991, Wrongful Access to Computers.

Federal Procedure, Lawyers Edition § 22:1685, Money Laundering Cases; Fraudulent Use of Financial Institutions.

Immigration Law Service 2d § 13:8, Sharing by Federal Agencies of Information Relevant to Deportation Under the Enhanced Border Security and Visa Entry Reform Act of 2002 and the Usa Patriot Act.

McCarthy on Trademarks and Unfair Competition § 25:68.50, Phishing.

Newberg on Class Actions § 11:41, Criteria for Approval of Final Settlement.

Newberg on Class Actions § 14:10, Hybrid Class Actions.

Patent Law Fundamentals § 4:1, Sources and Characteristics of Trade Secret Law.

Patent Law Fundamentals § 4:18, Unfair (Improper) Means--Crime--Under Federal Law.

Patent Law Fundamentals App. 4(B), Economic Espionage Act Cases.

Securities Crimes App 56, Sentencing Guidelines.

Securities Litigation: Damages § 5:12, Securities Fraud on the Internet.

Trade Secrets Law App P, Economic Espionage Act of 1996 (With Legislative History) (18 U.S.C.A. §§ 1831-1839).

NOTES OF DECISIONS

Agent 12
Constitutionality 1
Elements of civil action 8
Fraud 10
Injunction 9
Intent 3
Limit on claims 11
Limitations 6
Loss or damage 4
Pleading 6a

Protected computer 14
 Review 7
 Thing of value 5
 Third party computer, unauthorized access or use 2a
 Trafficking 13
 Unauthorized access or use 2-2a
 Unauthorized access or use - Third party computer 2a

1. Constitutionality

Application of statute prohibiting intentional interference with computer-related systems used in interstate commerce to defendant who interfered with city's computer-based communications systems used for police, fire, ambulance, and other emergency communications did not violate due process; statute itself gave all the notice that the Constitution required. *U.S. v. Mitra*, C.A.7 (Wis.) 2005, 405 F.3d 492, on remand 2005 WL 1181954, certiorari denied 126 S.Ct. 596, 546 U.S. 979, 163 L.Ed.2d 464. Constitutional Law ⚡ 4509(1); Telecommunications ⚡ 1314

Fact that computer fraud statute does not have mens rearequirement for damages element of offense does not render such statute unconstitutional. *U.S. v. Sablan*, C.A.9 (Guam) 1996, 92 F.3d 865. Malicious Mischief ⚡ 1

Exercise of personal jurisdiction over non-resident customers of computer consultant in consultant's suit for breach of contract and violations of computer fraud statute, Racketeer Influenced and Corrupt Organizations Act (RICO) and Georgia Trade Secrets Act comported with fair play and substantial justice; burden on customers in defending suit in another state was minimal in light of modern transit, consultant was resident of forum state and had strong interest in obtaining convenient and effective relief, and forum state had strong interest in protecting residents from misappropriation of computer data, technology and trade secrets. *Peridyne Technology Solutions, LLC v. Matheson Fast Freight, Inc.*, N.D.Ga.2000, 117 F.Supp.2d 1366. Constitutional Law ⚡ 3965(5); Federal Courts ⚡ 76.25; Federal Courts ⚡ 76.30; Federal Courts ⚡ 76.35

2. Unauthorized access or use

Anti-Injunction Act barred federal court, in employer's action against employee for alleged violation of the federal Computer Fraud and Abuse Act, from enjoining employee's Delaware state court action seeking advancement of attorney fees and costs, absent indication that the Delaware court was hostile to the Act and would express that hostility by seeking to reexamine prior ruling that employer had stated a claim under the Act. *International Airport Centers, L.L.C. v. Citrin*, C.A.7 (Ill.) 2006, 455 F.3d 749. Courts ⚡ 508(2.1)

Employee allegedly caused the "transmission" of a program resulting in damage to a protected computer, and "intentionally accessed" the computer "without authorization," or "exceeding authorization," in violation of the Computer Fraud and Abuse Act, by allegedly installing a secure-erasure program on his employer's computer; program was installed, either by downloading it from Internet onto employer's computer or by copying program from a disk onto computer, program caused permanent deletion of employer's files, and employee's authorized access to the computer terminated when he quit his employment in violation of his employment contract and re-

solved to destroy the files. *International Airport Centers, L.L.C. v. Citrin*, C.A.7 (Ill.) 2006, 440 F.3d 418, on subsequent appeal 455 F.3d 749. Telecommunications ↪ 1342

Defendant's interference with computer-based radio system used by city for police, fire, ambulance, and other emergency communications violated statute prohibiting intentional interference with computer-related systems used in interstate commerce. *U.S. v. Mitra*, C.A.7 (Wis.) 2005, 405 F.3d 492, on remand 2005 WL 1181954, certiorari denied 126 S.Ct. 596, 546 U.S. 979, 163 L.Ed.2d 464. Telecommunications ↪ 1348

Especially aggressive prophylactic injunction, permanently barring Computer Fraud and Abuse Act defendant's future access of plaintiff's website was not overbroad, given defendant's belligerent violation of temporary restraining order and preliminary injunction during litigation and its executives' lies in their depositions. *Creative Computing v. Getloaded.com LLC*, C.A.9 (Idaho) 2004, 386 F.3d 930. Injunction ↪ 189

Competitor's use of "scraper" computer software program to systematically and rapidly glean prices from tour company's website, in order to allow systematic undercutting of those prices, "exceeded authorized access" within meaning of Computer Fraud and Abuse Act (CFAA), as required to support company's civil enforcement action against competitor and its executives, assuming program's speed and efficiency depended on competitor's executive's breach of broad confidentiality agreement with company, his former employer; executive allegedly used his knowledge of company's proprietary codes to facilitate program's creation, contrary to agreement's prohibition against "use [of] such... information for employee's own benefit or for the benefit of any other person or business entity." *EF Cultural Travel BV v. Explorica, Inc.*, C.A.1 (Mass.) 2001, 274 F.3d 577. Telecommunications ↪ 1342

Defendant's transmission of computer "worm" constituted accessing federal interest computer without authorization under statute punishing anyone who intentionally accesses without authorization federal interest computers and damages or prevents authorized use of information in those computers causing loss of \$1,000 or more; defendant used computer program that transfers and receives electronic mail and program that permits person to obtain limited information about users of another computer to release "worm" into group of national networks that connected university, governmental, and military computers around the country and use of those features was not in any way related to their intended function. *U.S. v. Morris*, C.A.2 (N.Y.) 1991, 928 F.2d 504, certiorari denied 112 S.Ct. 72, 502 U.S. 817, 116 L.Ed.2d 46. Malicious Mischief ↪ 1; Telecommunications ↪ 1348

Hotel licensee violated the Computer Fraud and Abuse Act (CFAA) by attempting on numerous occasions within a one-year period to intentionally access without authorization licensor's protected computers located both within and outside of the United States, attempting to access remote computers within licensor's protected network, spoofing of licensor's computers, causing congestion on the licensor's VPN device, thereby impairing the availability of that computer to other systems in the network, and by intentionally accessing licensor's protected computers and thereby obtaining information of value in the form of confidential customer and financial data. *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, S.D.Fla.2003, 267 F.Supp.2d 1268, affirmed in part, reversed in part 138 Fed.Appx. 297, 2005 WL 850304, rehearing and rehearing en banc denied 163 Fed.Appx. 849, 2005 WL 2487946. Telecommunications ↪ 1342

Employee's acquisition of employer's confidential information prior to resigning employment for a new position with employer's competitor was not "without authorization" or in a manner that "exceeded authorized access," so as to give rise to civil cause of action under Computer Fraud and Abuse Act, where employee was authorized to initially access the computer he used at employer's place of business, and employee was permitted to view the specific files he allegedly e-mailed to himself. *Shamrock Foods Co. v. Gast*, D.Ariz.2008, 535 F.Supp.2d 962. Telecommunications ↪ 1342

On motion for preliminary injunction, condominium property management company had substantial likelihood of success on Computer Fraud and Abuse Act (CFAA) claim that former employee exceeded her authorization by downloading various files from company's computer system prior to leaving company for new job with company's competitor; company had right to control and define authorization to access its systems and files that employee downloaded were not necessary for employee's remaining business purposes. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications ↪ 903


Employees' accessing confidential information on workplace computers of employer, a pharmaceutical care provider, could not constitute access to protected computer "without authorization" under Computer Fraud and Abuse Act (CFAA), since employees as part of their jobs had limited access to employer's computer systems; however, employees' alleged accessing of reports that were outside scope of their duties, and e-mailing of confidential information to their personal accounts, constituted "exceeding authorized access" under CFAA and thus were cognizable under separate provisions of Act. *US Bioservices Corp. v. Lugo*, D.Kan.2009, 595 F.Supp.2d 1189. Telecommunications ↪ 1342


Sootblower manufacturer's former service manager was authorized to initially access manufacturer's computers and had password access to obtain specific information later disclosed to competitor, and thus did not access information on manufacturer's network without authorization or in a manner that exceeded his authorized access in violation of Computer Fraud and Abuse Act (CFAA), as required for manufacturer's claims against competitor and former manager under CFAA. *Diamond Power Intern., Inc. v. Davidson*, N.D.Ga.2007, 540 F.Supp.2d 1322. Telecommunications ↪ 1342


Former employer's allegation that employee intentionally accessed employer's database without authorization and/or exceeded her authorized access, and transferred information outside of employer to her own possession, and misappropriated and obtained valuable confidential, proprietary and trade secret information belonging to employer was sufficient to allege that employee was without authorization to access information, as required to state claim under Computer Fraud and Abuse Act (CFAA). *Modis, Inc. v. Bardelli*, D.Conn.2008, 531 F.Supp.2d 314. Telecommunications ↪ 1342


Former chief executive officer (CEO) had not been authorized to take proprietary information and delete relevant electronic files, for purpose of claim under Computer Fraud and Abuse Act (CFAA), although CEO deleted files while still officer and director of corporation; CEO breached his duty of loyalty and terminated his agency relationship to company when he decided to delete all information from corporation's server and his company computer night before his termination and after knowing that he was being asked to step down and give up his duties. *ViChip Corp. v. Lee*, N.D.Cal.2006, 438 F.Supp.2d 1087. Corporations ↪ 314(1); Telecommunications


tions  1342


There was insufficient evidence to support software developer's claim that its former joint venturer had accessed its computers without authority through use of remote access program, in violation of Computer Fraud and Abuse Act, despite developer's contention that venturer had sent "Trojan Horse" to its desktop computer in order to destroy evidence of its unauthorized access; there was no expert opinion evidence based on parties' respective forensic examinations of computers to demonstrate either unauthorized access in general or any access by venturer leading to destruction of developer's software or hardware. *Expert Business Systems, LLC v. BI4CE, Inc.*, D.Md.2006, 411 F.Supp.2d 601, affirmed 233 Fed.Appx. 251, 2007 WL 1381595. Telecommunications  1346

Software developer's attempts, in concert with consulting firm, to perform comparative analysis of competitor's product did not violate Computer Fraud and Abuse Act (CFAA), even though consultant breached licensing agreements with competitor restricting third parties' access to its materials, where consultant gave developer permission to access its server to view and download competitor's materials. *SecureInfo Corp. v. Telos Corp.*, E.D.Va.2005, 387 F.Supp.2d 593. Telecommunications  1342

Provider of advertising tracking services, which utilized Internet website, could proceed against competitor under Computer Fraud and Abuse Act provision forbidding obtaining of information from protected computer involved in interstate or foreign communication through intentional and unauthorized access, despite competitor's claim that there was no civil action for violation of provision. *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, S.D.N.Y.2004, 307 F.Supp.2d 521, 70 U.S.P.Q.2d 1105. Telecommunications  1342

University, which offered Internet-based doctoral program in which private school's principal had enrolled, did not violate Computer Fraud and Abuse Act (CFAA) when it received information about school from principal as he prepared his dissertation; even if information had come from school's computers, university did not "access" school's computers within meaning of CFAA. *Role Models America, Inc. v. Jones*, D.Md.2004, 305 F.Supp.2d 564. Telecommunications  1342

Computer Fraud and Abuse Act (CFAA) authorized employer's use of the Act's civil remedies to sue former employees and their new companies for seeking a competitive edge through wrongful use of information from the former employer's computer system. *Pacific Aerospace & Electronics, Inc. v. Taylor*, E.D.Wash.2003, 295 F.Supp.2d 1188. Telecommunications  1342

Internet domain name registrant who used authorization codes provided by domain name registry operator's agent to register names with his registrar did not violate statute granting computer system operator civil remedy against unauthorized accessors, even though it was later determined that codes had been given to registrant in error; registrant did not directly access operator's system, and operator's subsequent "locking" of names in question was not sort of data availability impairment contemplated by statute. *Davies v. Afilius Ltd.*, M.D.Fla.2003, 293 F.Supp.2d 1265, 69 U.S.P.Q.2d 1143, affirmed 129 Fed.Appx. 598, 2005 WL 176983. Telecommunications  1342

Individual who, while residing in Russia, gained root access to business's computers in Connecticut obtained access to business's intangible property, for purposes of Computer Fraud and Abuse Act (CFAA), in Connecticut, even if data was moved from Connecticut computer to computer located in Russia, and thus federal court in Connecticut had subject matter jurisdiction over individual's prosecution. *U.S. v. Ivanov*, D.Conn.2001, 175 F.Supp.2d 367. Telecommunications ☞ 1348

Advertiser violated Computer Fraud and Abuse Act (CFAA) when e-mailers acting as its agent sent unsolicited bulk e-mail (UBE) to customers of internet services provider (ISP); access was not authorized, information was obtained from protected computers, and ISP sustained damages in excess of \$5,000 in single year. *America Online, Inc. v. National Health Care Discount, Inc.*, N.D.Iowa 2001, 174 F.Supp.2d 890. Telecommunications ☞ 1343

Internet dating service was entitled to temporary restraining order (TRO) prohibiting a former programmer from "hacking" the dating service's website and diverting its clients and users to a porn site; dating service had a likelihood of success on the merits of its claim that former programmer was responsible for alleged violations of the Computer Fraud and Abuse Act, and showed irreparable harm in the damage to the goodwill of its services, while programmer and operator of porn site would suffer no legitimate harm from issuance of TRO nor would the public. *YourNetDating, Inc. v. Mitchell*, N.D.Ill.2000, 88 F.Supp.2d 870. Injunction ☞ 138.24

Internet site operators' maintenance of membership with Internet service provider in order to use that membership to harvest e-mail addresses of provider's customers and send bulk e-mails to those customers, in violation of provider's terms of service, violated Computer Fraud and Abuse Act, which prohibits individuals from exceeding authorized access. *America Online, Inc. v. LCGM, Inc.*, E.D.Va.1998, 46 F.Supp.2d 444. Telecommunications ☞ 1342

Agency had reasonable cause to believe that employee, who had altered computer contracts, had committed crime, so as to invoke crime provision, even though employee claimed that alterations were not to defraud government, but only to show lack of security safeguards; relevant criminal statute only required proof of use of computer system for any unauthorized purpose. *Sawyer v. Department of Air Force*, M.S.P.B.1986, 31 M.S.P.R. 193. Merit Systems Protection ☞ 184

Eighteen-month sentence, upon conviction for accessing protected computer without authorization, did not violate *Apprendi* or *Ring*; no facts or aggravating factors were used to increase penalty beyond statutory maximum for offense of conviction. *Leung v. U.S.*, S.D.N.Y.2003, 2003 WL 22149526, Unreported. Jury ☞ 34(7); Sentencing And Punishment ☞ 322.5

2a. ---- Third party computer, unauthorized access or use

Use of a third party's computer to access a website, rather than one's own computer, does not prevent a claim under the Computer Fraud and Abuse Act (CFAA). *eBay Inc. v. Digital Point Solutions, Inc.*, N.D.Cal.2009, 608 F.Supp.2d 1156. Telecommunications ☞ 1342

3. Intent

The crime of accessing a protected computer without authorization and thereby obtaining information from that computer only requires proof that defendant intentionally accessed information from a protected computer, it does not require proof of intent to defraud nor proof that the defendant knew the value of the information obtained. *U.S. v. Willis*, C.A.10 (Okla.) 2007, 476 F.3d 1121, certiorari denied 127 S.Ct. 3025, 168 L.Ed.2d 744. Telecommunications 🔑 1348

Computer fraud statute did not require government to prove that defendant intentionally damaged computer files, but only that defendant intentionally accessed computer without authorization. *U.S. v. Sablan*, C.A.9 (Guam) 1996, 92 F.3d 865. Malicious Mischief 🔑 1

On motion for preliminary injunction, condominium property management company failed to show substantial likelihood of success on Computer Fraud and Abuse Act (CFAA) claim that former employee took files from company's computer system prior to leaving company for new job with company's competitor with intent to defraud company; rather, employee took files because she believed they would be useful to her personally in her new position. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications 🔑 903

Allegations that former employees intentionally accessed their former employer's protected computer, without authorization, and as a result of such conduct caused damage to employer by, among other things, obtaining its confidential and proprietary information for the benefit of employees' competing enterprise were sufficient to state claim for violation of the Computer Fraud and Abuse Act (CFAA). *Resource Center for Independent Living, Inc. v. Ability Resources, Inc.*, D.Kan.2008, 534 F.Supp.2d 1204. Telecommunications 🔑 1342

Copyright owner stated claim under Electronic Communications Privacy Act (ECPA), on allegations that customer "intentionally access[ed] without authorization, or intentionally exceed[ed] an authorization to access, the password-protected areas of [copyright owner's] Internet web site," obtained "access to electronic communications while such communications were in electronic storage on that web site, and disclos[ed] such communications to third parties [who were] not authorized to receive them, and conspir[ed], encourag[ed], aid[ed], abett[ed], and participat[ed] in efforts to do so." *Therapeutic Research Faculty v. NBTY, Inc.*, E.D.Cal.2007, 488 F.Supp.2d 991, 81 U.S.P.Q.2d 1723. Telecommunications 🔑 1439

Allegations in plaintiff's complaint, that unlawful attempts to gain access to its computer server were made from computer manufacture's facility with equipment owned and operated by manufacturer and were directed by manufacturer's employees or agents, were insufficient to plead intentional conduct by manufacturer, as required to state a claim against manufacturer for violations of Computer Fraud and Abuse Act, Stored Wire and Electronic Communications Act, and Federal Wiretap Act; plaintiff did not allege that manufacturer authorized any person to attack or otherwise obtain unauthorized access to its computer systems. *Butera & Andrews v. International Business Machines Corp.*, D.D.C.2006, 456 F.Supp.2d 104. Telecommunications 🔑 1342; Telecommunications 🔑 1439

Allegation that web site operator intentionally placed “cookies” on visiting users' computers for purpose of monitoring their web activity was sufficient to satisfy scienter element of claim that operator violated statute proscribing intentional computer access without authorization and knowing transmission of program without authorization. *In re Intuit Privacy Litigation*, C.D.Cal.2001, 138 F.Supp.2d 1272. Telecommunications 🔑 1342

4. Loss or damage

Record supported district court's determination that it was foreseeable to defendant that his dissemination of username and password to secure website which provided financial information on individuals for debt collection would have value of between \$10,000 and \$30,000, for purposes of determining the amount of loss associated with his offense of aiding and abetting the accessing without authorization of a protected computer; defendant gave the information to his methamphetamine supplier in exchange for better price on drugs, when defendant gave information to another person she assured defendant she would take care of him later, and defendant was well aware that information available on website was valuable. *U.S. v. Willis*, C.A.10 (Okla.) 2007, 476 F.3d 1121, certiorari denied 127 S.Ct. 3025, 168 L.Ed.2d 744. Sentencing And Punishment 🔑 978

Employee's entitlement under his employment contract to an advance for the attorneys' fees and other expenses that he was incurring to defend against employer's suit for violation of the federal Computer Fraud and Abuse Act was independent of the merits of the suit, and thus was not a compulsory counterclaim. *International Airport Centers, L.L.C. v. Citrin*, C.A.7 (Ill.) 2006, 455 F.3d 749. Federal Civil Procedure 🔑 777

Losses sustained by contractor hired to manage secure computer system of defendant's former employer could be considered when determining whether defendant's damage to the system exceeded \$5,000, in violation of the Computer Fraud and Abuse Act (CFAA); statute did not restrict consideration of losses to only the person who owned the computer system. *U.S. v. Millot*, C.A.8 (Mo.) 2006, 433 F.3d 1057. Telecommunications 🔑 1348

Claim under Computer Fraud and Abuse Act (CFAA) for knowingly accessing a protected computer without authorization and with intent to defraud was actionable under CFAA's civil remedy provision, where plaintiffs alleged their loss exceeded \$5,000. *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC.*, C.A.3 (N.J.) 2005, 428 F.3d 504. Telecommunications 🔑 1342

Awards of \$150,000 for each of three violations of Computer Fraud and Abuse Act, and \$60,000 for violation of Idaho Trade Secrets Act, were supported by evidence; although victim had lost on its copyright and Lanham Act claims, and its expert had not attempted to segregate its damages according to each claim, jury was told that it could accept all, part, or none of expert's testimony, and it had other evidence aside from that testimony from which it could reach reasonable conclusion about amount of damages. *Creative Computing v. Getloaded.com LLC*, C.A.9 (Idaho) 2004, 386 F.3d 930. Telecommunications 🔑 1345

Term “individual,” as used in statute that prohibits any person from knowingly causing damage, without authorization, to protected computer, and that defines “damage” as any impairment which causes loss aggregating at least \$5,000 to one or more individuals, is broad enough to include corporations as well as natural persons; statute criminalizes computer crime that damages natural persons and corporations alike. *U.S. v. Middleton*, C.A.9

(Cal.) 2000, 231 F.3d 1207. Malicious Mischief ☞ 1

Statute which punishes anyone who intentionally accesses without authorization federal interest computers and damages or prevents authorized use of information in those computers causing loss of \$1,000 or more does not require Government to demonstrate that defendant intentionally prevented authorized use and thereby caused loss. *U.S. v. Morris*, C.A.2 (N.Y.) 1991, 928 F.2d 504, certiorari denied 112 S.Ct. 72, 502 U.S. 817, 116 L.Ed.2d 46. Malicious Mischief ☞ 1; Telecommunications ☞ 1348

Hotel licensee's spoofing of licensor's computers, in and of itself, constituted the unlawful, intentional transmission of a program, code or command that caused damage within meaning of Computer Fraud and Abuse Act (CFAA). *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, S.D.Fla.2003, 267 F.Supp.2d 1268, affirmed in part, reversed in part 138 Fed.Appx. 297, 2005 WL 850304, rehearing and rehearing en banc denied 163 Fed.Appx. 849, 2005 WL 2487946. Telecommunications ☞ 1342

Lost revenue from stolen trade secrets was not "damage" or "loss" which corporation could recover on claim under Computer Fraud and Abuse Act (CFAA) against former employees who allegedly accessed corporation's computer network without authorization, stole trade secrets, and gave them to competitor; there was no impairment to corporation's network or data as a result of alleged theft, corporation did not suffer any damage related to responding to theft or conducting a damage assessment, and corporation did not lose revenue or incur costs because of interruption of network service. *Andritz, Inc. v. Southern Maintenance Contractor, LLC*, M.D.Ga.2009, 626 F.Supp.2d 1264. Telecommunications ☞ 1342

Real estate information services provider, which owned an online database with photos of real property, adequately alleged loss, as required to state claim for violation of the Computer Fraud and Abuse Act, by alleging loss of revenue from license fees due to users' unauthorized use of its database and that users' unauthorized access caused damage to provider amounting in an aggregate loss of over \$5,000 during a one-year period. *CoStar Realty Information, Inc. v. Field*, D.Md.2009, 612 F.Supp.2d 660. Telecommunications ☞ 1345

Plaintiff who had been prosecuted in case alleging international conspiracy to distribute illegal prescription drugs had no civil remedy against federal agents and assistant United States attorneys for violation of the Computer Fraud and Abuse Act (CFAA); plaintiff did not allege at least \$5000 in economic damages related to alleged violation of the CFAA. *Bansal v. Russ*, E.D.Pa.2007, 513 F.Supp.2d 264. Telecommunications ☞ 1342

Employer's allegations that employee damaged employer by wrongfully and intentionally accessing its computer system to obtain confidential information and computer programs and software failed to adequately plead loss, as required to state a claim for violation of Computer Fraud and Abuse Act (CFAA). *Cenveo Corp. v. Celum-Solutions Software GMBH & Co KG*, D.Minn.2007, 504 F.Supp.2d 574. Telecommunications ☞ 1342

Copyright owner stated that it suffered loss of \$5,000 or more under Computer Fraud and Abuse Act (CFAA), on allegations that customer breached single user license agreement by pasting of text from copyrighted work into email, sending of emails to unauthorized users, and "full corporate license for [customer] and its subsidiaries

would cost approximately forty thousand dollars per year,” as opposed to under \$100 for “an annual single user limited-purpose subscription.” *Therapeutic Research Faculty v. NBTY, Inc.*, E.D.Cal.2007, 488 F.Supp.2d 991, 81 U.S.P.Q.2d 1723. Copyrights And Intellectual Property 🔑 82

Manufacturer, alleging competitor's induced deletion of files on third-parties' computers that contained manufacturer's confidential proprietary information, lacked standing to assert civil claim under Computer Fraud and Abuse Act (CFAA), absent showing that it had suffered loss of at least \$5,000 in value; neither response costs incurred by manufacturer, which were unrelated to any computer investigation or repair, nor revenue lost as result of competitor's alleged misappropriation of information in files, constituted “loss” within meaning of statute. *Nexans Wires S.A. v. Sark-USA, Inc.*, S.D.N.Y.2004, 319 F.Supp.2d 468, affirmed 166 Fed.Appx. 559, 2006 WL 328292. Telecommunications 🔑 1345

Provider of advertising tracking services, which utilized Internet website, alleged loss as required for claim under Computer Fraud and Abuse Act, by asserting that competitor's copying of forms used for storage of information forced provider to incur costs of more than \$5,000 in damage assessment and remedial measures. *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*, S.D.N.Y.2004, 307 F.Supp.2d 521, 70 U.S.P.Q.2d 1105. Telecommunications 🔑 1342

For purposes of obtaining preliminary injunctive relief, balance of harm tipped decidedly toward employer, which brought action against former employees and their new company for misappropriation of trade secrets; employer provided undisputed evidence that customer list and proprietary information has been provided to new company's sales representative in an effort to solicit business in competition with employer. *Pacific Aerospace & Electronics, Inc. v. Taylor*, E.D.Wash.2003, 295 F.Supp.2d 1188. Injunction 🔑 138.33

Absence of evidence that computer network belonging to developer of automated stock-trading computer systems was damaged in any quantifiable amount by alleged unauthorized accessing of network by custom software company and its owner precluded developer's recovery under provision of Computer Fraud and Abuse Act (CFAA) allowing for civil action based on violation causing loss during one-year period aggregating at least \$5,000 in value. *Pearl Investments, LLC v. Standard I/O, Inc.*, D.Me.2003, 257 F.Supp.2d 326. Telecommunications 🔑 1342

Customer's civil claim under Computer Fraud and Abuse Act (CFAA) based on purported defect in floppy diskette controllers (FDCs) in manufacturer's computers required allegation that defect caused \$5,000 damage to each protected computer, not \$5,000 damage to protected computers in aggregate. *Hayes v. Packard Bell, Nec.*, E.D.Tex.2001, 193 F.Supp.2d 910. Telecommunications 🔑 1342

Losses suffered by unnamed members of proposed class made up of buyers of allegedly defective computers could not be used to satisfy threshold money damages requirement in Computer Fraud and Abuse Act (CFAA) civil action. *Thurmond v. Compaq Computer Corp.*, E.D.Tex.2001, 171 F.Supp.2d 667. Telecommunications 🔑 1342

Each time Internet advertising company placed “cookie” on visiting user's computers for purpose of monitoring his or her web activity constituted separate “act” under Computer Fraud and Abuse Act (CFAA) provision setting \$5,000 threshold of damage for individual act in order to state valid cause of action. *Chance v. Avenue A, Inc.*, W.D.Wash.2001, 165 F.Supp.2d 1153. Telecommunications ☞ 1342

Employer engaged in self-storage business stated claim against competitor, for alleged damage to its computers arising from competitor's alleged receipt from former employees of trade secret information obtained in violation of Computer Fraud and Abuse Act (CFAA), despite claim that no damage occurred since information remained intact within computers; employer suffered loss in form of expenses incurred in modifying computers to preclude further data transfer. *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, W.D.Wash.2000, 119 F.Supp.2d 1121, 174 A.L.R. Fed. 655. Telecommunications ☞ 1342

Designer of allegedly defective microcode used in computer floppy-diskette controllers could be held liable, under Computer Fraud and Abuse Act provision prohibiting transmission of code which intentionally causes damage to protected computers, for third party's sales of computers incorporating controllers which contained defective code; designer could have reasonably anticipated such sales. *Shaw v. Toshiba America Information Systems, Inc.*, E.D.Tex.1999, 91 F.Supp.2d 926. Telecommunications ☞ 1342

Statute making it an offense to cause damage to a protected computer, by knowingly causing the transmission of a program, information, code, or command, resulting in a specified loss to one or more “individuals,” encompasses damage sustained by a business entity as well as by a natural person. *U.S. v. Middleton*, N.D.Cal.1999, 35 F.Supp.2d 1189. Malicious Mischief ☞ 1

5. Thing of value

Former employees' alleged improper access to their former employer's protected computer system did not violate the Computer Fraud and Abuse Act (CFAA) provision prohibiting accessing a protected computer system with intent to defraud to obtain something of value, absent evidence as to what, if any, information was actually viewed, let alone taken. *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC.*, C.A.3 (N.J.) 2005, 428 F.3d 504. Telecommunications ☞ 1342

Defendant could not be convicted of computer fraud in connection with his browsing of confidential taxpayer files, even though he exceeded authorized access to a federal interest computer, as he did not obtain “anything of value.” *U.S. v. Czubinski*, C.A.1 (Mass.) 1997, 106 F.3d 1069. Fraud ☞ 68

Internet service provider (ISP) was provided with something “of value,” under Computer Fraud and Abuse Act (CFAA) provision prohibiting receipt of anything “of value” after gaining of access to computer or exceeding authority in furtherance of fraud, when ISP allegedly deprived competitor of subscribers' custom and trade by distributing software program that prohibited or discouraged subscribers' use of competitor's software. *In re America Online, Inc.*, S.D.Fla.2001, 168 F.Supp.2d 1359. Telecommunications ☞ 1342

6. Limitations

Cause of action under Computer Fraud and Abuse Act (CFAA) accrued, and two-year limitations period began to run, when government relations and analysis firm alleged it suffered loss arising from customer-turned-competitor accessing firm's website subscription services "without authorization," in violation of CFAA. *State Analysis, Inc. v. American Financial Services Assoc.*, E.D.Va.2009, 621 F.Supp.2d 309. Limitation Of Actions ⚡ 58(1)

Two year statute of limitations on filing of Computer Fraud and Abuse Act (CFAA) claim was not equitably tolled where, at time plaintiff learned all additional facts necessary to file claim, limitations period still had seven months left but plaintiff waited year and a half to file claim. *Egilman v. Keller & Heckman, LLP.*, D.D.C.2005, 401 F.Supp.2d 105, 77 U.S.P.Q.2d 1070. Limitation Of Actions ⚡ 104.5

6a. Pleading

Allegations that former customer-turned-competitor of government relations and analysis firm accessed firm's website using usernames and passwords that did not belong to it, and that competitor was not authorized to use firm's subscription services, was sufficient to allege that competitor acted "without authorization" in accessing firm's website, as required for firm to state claim that competitor violated Computer Fraud and Abuse Act (CFAA). *State Analysis, Inc. v. American Financial Services Assoc.*, E.D.Va.2009, 621 F.Supp.2d 309. Telecommunications ⚡ 1342

Auction website operator's allegation that advertising affiliate caused users to access website solely to corrupt operator's advertising affiliate data was sufficient to state a claim of unauthorized access against affiliate in violation of the Computer Fraud and Abuse Act (CFAA). *eBay Inc. v. Digital Point Solutions, Inc.*, N.D.Cal.2009, 608 F.Supp.2d 1156. Telecommunications ⚡ 1342

Former employer's factual allegations concerning office locations in two different states set forth plausible claim that former employee engaged in an interstate or foreign communication, and that computer she used was a protected computer used in interstate or foreign commerce or communication, for purposes of employer's Computer Fraud and Abuse Act (CFAA) claims against former employee. *Modis, Inc. v. Bardelli*, D.Conn.2008, 531 F.Supp.2d 314. Telecommunications ⚡ 1342

7. Review

Upon appeal from grant of motion to dismiss former employer's action against former employee, for violation of the Computer Fraud and Abuse Act, in connection with employee's alleged installation of secure-erasure program to destroy employer's files on employer's computer, Court of Appeals would not determine whether files destroyed were confidential, as would arguably be permitted by employment contract authorizing employee to return or destroy confidential information in the computer when he ceased his employment. *International Airport Centers, L.L.C. v. Citrin*, C.A.7 (Ill.) 2006, 440 F.3d 418, on subsequent appeal 455 F.3d 749. Federal Courts ⚡ 753

8. Elements of civil action

Condominium property management company's former employee did not act in bad faith in accessing files she had downloaded from company's computer system prior to leaving company for new job with company's competitor after commencement of company's Computer Fraud and Abuse Act (CFAA) action against employee and competitor, which resulted in destruction of certain embedded metadata within files, and thus adverse inference that files were taken with intention to use information in new employment was not warranted; employee did not know that accessing files would result in destruction of data, and thus did not rise to level of spoliation of evidence. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications ☞ 1346

Former client of government relations and analysis firm did not violate Computer Fraud and Abuse Act (CFAA) in using database and custom reports on firm's website, since client never went beyond areas on website that firm authorized client to access so as to constitute access "without authorization," and client did not obtain or alter information from website it was not entitled to so as to "exceed authorization" in using site. *State Analysis, Inc. v. American Financial Services Assoc.*, E.D.Va.2009, 621 F.Supp.2d 309. Telecommunications ☞ 1342

Civil actions brought for violation of Computer Fraud and Abuse Act (CFAA) may only be based on alleged violations of CFAA provision prohibiting the knowing transmission of a program, information, code, or command that intentionally causes damage without authorization to a protected computer. *Cenveo Corp. v. CelumSolutions Software GMBH & Co KG*, D.Minn.2007, 504 F.Supp.2d 574. Telecommunications ☞ 1342

9. Injunction

Employers were not entitled to preliminary injunction requiring former employees to return any information that they deleted from employers' servers, barring former employees from using or disclosing employer's trade secrets and enjoining them from continuing to work for any direct competitor; damage done to employers by the alleged improper acquisition of confidential information would be difficult to quantify, if employers proved claims under the state and federal computer crimes statutes, their remedy was limited to monetary damages unless they could prove ongoing acts causing harm to their computers or to their business interests, and balance of harms tipped in favor of former employees, who would be barred from continuing to work for competitor if injunction was granted. *Maxpower Corp. v. Abraham*, W.D.Wis.2008, 557 F.Supp.2d 955, reconsideration denied 2008 WL 2953909. Injunction ☞ 138.31; Injunction ☞ 138.33; Telecommunications ☞ 1345

10. Fraud

Fraud under the Computer Fraud and Abuse Act (CFAA) only requires a showing of unlawful access; there is no need to plead the elements of common law fraud to state a claim under the Act. *eBay Inc. v. Digital Point Solutions, Inc.*, N.D.Cal.2009, 608 F.Supp.2d 1156. Telecommunications ☞ 1342

11. Limit on claims

Condominium property management company's costs for forensic investigation of computer system after employee, who allegedly acted as agent of company's competitor and downloaded proprietary information from company's computer system prior to leaving company for new job with competitor, did not result from interrup-

tion of service, and thus company failed to meet \$5,000 jurisdictional limit in its Computer Fraud and Abuse Act (CFAA) action against competitor and former employee; costs did not constitute "loss" under plain language of CFAA provision, which required that all loss must be result of interruption of service. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications ☞ 1342

Condominium property management company's computer system constituted a "protected computer" under Computer Fraud and Abuse Act (CFAA) provision governing fraud and related activity in connection with computers, in action against competitor and former employee for taking proprietary information from company's computers, despite argument that company's system connected its offices only within Florida; company used its internet connection to communicate with its largest shareholder, which was based outside Florida. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications ☞ 1342

12. Agent

Condominium property management company's employee was not acting as an agent of company's competitor when she downloaded files from company's computer system prior to leaving company for new job with competitor, thus precluding preliminary injunctive relief on company's Computer Fraud and Abuse Act (CFAA) claim against competitor; competitor lacked knowledge of employee's actions and did not give even tacit approval for them. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications ☞ 903

13. Trafficking

Allegations that former customer-turned-competitor of government relations and analysis firm received passwords to database and custom reports on firm's website from firm's former client failed to state claim that competitor "trafficked" firm's password through which its computer could be accessed without authorization, as would violate Computer Fraud and Abuse Act (CFAA); complaint alleged that competitor received passwords from former client without authorization, which did not constitute "trafficking" under CFAA. *State Analysis, Inc. v. American Financial Services Assoc.*, E.D.Va.2009, 621 F.Supp.2d 309. Telecommunications ☞ 1342

14. Protected computer

Condominium property management company's computer system constituted a "protected computer" under Computer Fraud and Abuse Act (CFAA) provision governing fraud and related activity in connection with computers, in action against competitor and former employee for taking proprietary information from company's computers, despite argument that company's system connected its offices only within Florida; company used its internet connection to communicate with its largest shareholder, which was based outside Florida. *Continental Group, Inc. v. KW Property Management, LLC*, S.D.Fla.2009, 622 F.Supp.2d 1357. Telecommunications ☞ 1342

18 U.S.C.A. § 1030, 18 USCA § 1030
Current through P.L. 111-82 approved 10-26-09

Westlaw. (C) 2009 Thomson Reuters. No Claim to Orig. U.S. Govt. Works.

END OF DOCUMENT