

ASSEMBLY BILL

No. 22

Introduced by Assembly Member Torres

December 1, 2008

An act to amend Section 502 of the Penal Code, relating to computer hacking.

LEGISLATIVE COUNSEL'S DIGEST

AB 22, as introduced, Torres. Computer hacking: financial institutions.

Existing law provides that any person who, among other things, knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, as defined, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network, is punishable by a fine not exceeding \$10,000, or by imprisonment in the state prison for 16 months, or 2 or 3 years, or by both that fine and imprisonment, or by a fine not exceeding \$5,000, or by imprisonment in a county jail not exceeding one year, or by both that fine and imprisonment.

This bill would provide that in the case of a violation involving the computer, computer system, or computer network of a bank, savings and loan, credit card issuer, or other financial institution, the fine for the felony conviction would be increased, not to exceed \$50,000.

Vote: majority. Appropriation: no. Fiscal committee: no.
State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Section 502 of the Penal Code is amended to read:

502. (a) It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems. The Legislature finds and declares that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data.

The Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data.

(b) For the purposes of this section, the following terms have the following meanings:

(1) "Access" means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network.

(2) "Computer network" means any system that provides communications between one or more computer systems and input/output devices including, but not limited to, display terminals and printers connected by telecommunication facilities.

(3) "Computer program or software" means a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(4) "Computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.

(5) "Computer system" means a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs,

1 electronic instructions, input data, and output data, that performs
2 functions including, but not limited to, logic, arithmetic, data
3 storage and retrieval, communication, and control.

4 (6) “Data” means a representation of information, knowledge,
5 facts, concepts, computer software, computer programs or
6 instructions. Data may be in any form, in storage media, or as
7 stored in the memory of the computer or in transit or presented on
8 a display device.

9 (7) “Supporting documentation” includes, but is not limited to,
10 all information, in any form, pertaining to the design, construction,
11 classification, implementation, use, or modification of a computer,
12 computer system, computer network, computer program, or
13 computer software, which information is not generally available
14 to the public and is necessary for the operation of a computer,
15 computer system, computer network, computer program, or
16 computer software.

17 (8) “Injury” means any alteration, deletion, damage, or
18 destruction of a computer system, computer network, computer
19 program, or data caused by the access, or the denial of access to
20 legitimate users of a computer system, network, or program.

21 (9) “Victim expenditure” means any expenditure reasonably
22 and necessarily incurred by the owner or lessee to verify that a
23 computer system, computer network, computer program, or data
24 was or was not altered, deleted, damaged, or destroyed by the
25 access.

26 (10) “Computer contaminant” means any set of computer
27 instructions that are designed to modify, damage, destroy, record,
28 or transmit information within a computer, computer system, or
29 computer network without the intent or permission of the owner
30 of the information. They include, but are not limited to, a group
31 of computer instructions commonly called viruses or worms, that
32 are self-replicating or self-propagating and are designed to
33 contaminate other computer programs or computer data, consume
34 computer resources, modify, destroy, record, or transmit data, or
35 in some other fashion usurp the normal operation of the computer,
36 computer system, or computer network.

37 (11) “Internet domain name” means a globally unique,
38 hierarchical reference to an Internet host or service, assigned
39 through centralized Internet naming authorities, comprising a series

1 of character strings separated by periods, with the rightmost
2 character string specifying the top of the hierarchy.

3 (c) Except as provided in subdivision (h), any person who
4 commits any of the following acts is guilty of a public offense:

5 (1) Knowingly accesses and without permission alters, damages,
6 deletes, destroys, or otherwise uses any data, computer, computer
7 system, or computer network in order to either (A) devise or
8 execute any scheme or artifice to defraud, deceive, or extort, or
9 (B) wrongfully control or obtain money, property, or data.

10 (2) Knowingly accesses and without permission takes, copies,
11 or makes use of any data from a computer, computer system, or
12 computer network, or takes or copies any supporting
13 documentation, whether existing or residing internal or external
14 to a computer, computer system, or computer network.

15 (3) Knowingly and without permission uses or causes to be used
16 computer services.

17 (4) Knowingly accesses and without permission adds, alters,
18 damages, deletes, or destroys any data, computer software, or
19 computer programs which reside or exist internal or external to a
20 computer, computer system, or computer network.

21 (5) Knowingly and without permission disrupts or causes the
22 disruption of computer services or denies or causes the denial of
23 computer services to an authorized user of a computer, computer
24 system, or computer network.

25 (6) Knowingly and without permission provides or assists in
26 providing a means of accessing a computer, computer system, or
27 computer network in violation of this section.

28 (7) Knowingly and without permission accesses or causes to be
29 accessed any computer, computer system, or computer network.

30 (8) Knowingly introduces any computer contaminant into any
31 computer, computer system, or computer network.

32 (9) Knowingly and without permission uses the Internet domain
33 name of another individual, corporation, or entity in connection
34 with the sending of one or more electronic mail messages, and
35 thereby damages or causes damage to a computer, computer
36 system, or computer network.

37 (d) (1) (A) Any person who violates any of the provisions of
38 paragraph (1), ~~(2)~~, (4), or (5) of subdivision (c) is punishable by
39 a fine not exceeding ten thousand dollars (\$10,000), or by
40 imprisonment in the state prison for 16 months, or two or three

1 years, or by both that fine and imprisonment, or by a fine not
2 exceeding five thousand dollars (\$5,000), or by imprisonment in
3 a county jail not exceeding one year, or by both that fine and
4 imprisonment.

5 *(B) A violation of paragraph (2) of subdivision (c) is punishable*
6 *by a fine not exceeding fifty thousand dollars (\$50,000), or by*
7 *imprisonment in the state prison for 16 months, or two or three*
8 *years, or by both that fine and imprisonment, or by a fine not*
9 *exceeding five thousand dollars (\$5,000), or by imprisonment in*
10 *a county jail not exceeding one year, or by both that fine and*
11 *imprisonment.*

12 (2) Any person who violates paragraph (3) of subdivision (c)
13 is punishable as follows:

14 (A) For the first violation that does not result in injury, and
15 where the value of the computer services used does not exceed
16 four hundred dollars (\$400), by a fine not exceeding five thousand
17 dollars (\$5,000), or by imprisonment in a county jail not exceeding
18 one year, or by both that fine and imprisonment.

19 (B) For any violation that results in a victim expenditure in an
20 amount greater than five thousand dollars (\$5,000) or in an injury,
21 or if the value of the computer services used exceeds four hundred
22 dollars (\$400), or for any second or subsequent violation, by a fine
23 not exceeding ten thousand dollars (\$10,000), or by imprisonment
24 in the state prison for 16 months, or two or three years, or by both
25 that fine and imprisonment, or by a fine not exceeding five
26 thousand dollars (\$5,000), or by imprisonment in a county jail not
27 exceeding one year, or by both that fine and imprisonment.

28 (3) Any person who violates paragraph (6) or (7) of subdivision
29 (c) is punishable as follows:

30 (A) For a first violation that does not result in injury, an
31 infraction punishable by a fine not exceeding one thousand dollars
32 (\$1,000).

33 (B) For any violation that results in a victim expenditure in an
34 amount not greater than five thousand dollars (\$5,000), or for a
35 second or subsequent violation, by a fine not exceeding five
36 thousand dollars (\$5,000), or by imprisonment in a county jail not
37 exceeding one year, or by both that fine and imprisonment.

38 (C) For any violation that results in a victim expenditure in an
39 amount greater than five thousand dollars (\$5,000), by a fine not
40 exceeding ten thousand dollars (\$10,000), or by imprisonment in

1 the state prison for 16 months, or two or three years, or by both
2 that fine and imprisonment, or by a fine not exceeding five
3 thousand dollars (\$5,000), or by imprisonment in a county jail not
4 exceeding one year, or by both that fine and imprisonment.

5 (4) Any person who violates paragraph (8) of subdivision (c)
6 is punishable as follows:

7 (A) For a first violation that does not result in injury, a
8 misdemeanor punishable by a fine not exceeding five thousand
9 dollars (\$5,000), or by imprisonment in a county jail not exceeding
10 one year, or by both that fine and imprisonment.

11 (B) For any violation that results in injury, or for a second or
12 subsequent violation, by a fine not exceeding ten thousand dollars
13 (\$10,000), or by imprisonment in a county jail not exceeding one
14 year, or in the state prison, or by both that fine and imprisonment.

15 (5) Any person who violates paragraph (9) of subdivision (c)
16 is punishable as follows:

17 (A) For a first violation that does not result in injury, an
18 infraction punishable by a fine not one thousand dollars.

19 (B) For any violation that results in injury, or for a second or
20 subsequent violation, by a fine not exceeding five thousand dollars
21 (\$5,000), or by imprisonment in a county jail not exceeding one
22 year, or by both that fine and imprisonment.

23 (e) (1) In addition to any other civil remedy available, the owner
24 or lessee of the computer, computer system, computer network,
25 computer program, or data who suffers damage or loss by reason
26 of a violation of any of the provisions of subdivision (c) may bring
27 a civil action against the violator for compensatory damages and
28 injunctive relief or other equitable relief. Compensatory damages
29 shall include any expenditure reasonably and necessarily incurred
30 by the owner or lessee to verify that a computer system, computer
31 network, computer program, or data was or was not altered,
32 damaged, or deleted by the access. For the purposes of actions
33 authorized by this subdivision, the conduct of an unemancipated
34 minor shall be imputed to the parent or legal guardian having
35 control or custody of the minor, pursuant to the provisions of
36 Section 1714.1 of the Civil Code.

37 (2) In any action brought pursuant to this subdivision the court
38 may award reasonable attorney's fees.

39 (3) A community college, state university, or academic
40 institution accredited in this state is required to include

1 computer-related crimes as a specific violation of college or
2 university student conduct policies and regulations that may subject
3 a student to disciplinary sanctions up to and including dismissal
4 from the academic institution. This paragraph shall not apply to
5 the University of California unless the Board of Regents adopts a
6 resolution to that effect.

7 (4) In any action brought pursuant to this subdivision for a
8 willful violation of the provisions of subdivision (c), where it is
9 proved by clear and convincing evidence that a defendant has been
10 guilty of oppression, fraud, or malice as defined in subdivision (c)
11 of Section 3294 of the Civil Code, the court may additionally award
12 punitive or exemplary damages.

13 (5) No action may be brought pursuant to this subdivision unless
14 it is initiated within three years of the date of the act complained
15 of, or the date of the discovery of the damage, whichever is later.

16 (f) This section shall not be construed to preclude the
17 applicability of any other provision of the criminal law of this state
18 which applies or may apply to any transaction, nor shall it make
19 illegal any employee labor relations activities that are within the
20 scope and protection of state or federal labor laws.

21 (g) Any computer, computer system, computer network, or any
22 software or data, owned by the defendant, that is used during the
23 commission of any public offense described in subdivision (c) or
24 any computer, owned by the defendant, which is used as a
25 repository for the storage of software or data illegally obtained in
26 violation of subdivision (c) shall be subject to forfeiture, as
27 specified in Section 502.01.

28 (h) (1) Subdivision (c) does not apply to punish any acts which
29 are committed by a person within the scope of his or her lawful
30 employment. For purposes of this section, a person acts within the
31 scope of his or her employment when he or she performs acts
32 which are reasonably necessary to the performance of his or her
33 work assignment.

34 (2) Paragraph (3) of subdivision (c) does not apply to penalize
35 any acts committed by a person acting outside of his or her lawful
36 employment, provided that the employee's activities do not cause
37 an injury, as defined in paragraph (8) of subdivision (b), to the
38 employer or another, or provided that the value of supplies or
39 computer services, as defined in paragraph (4) of subdivision (b),

1 which are used does not exceed an accumulated total of one
2 hundred dollars (\$100).

3 (i) No activity exempted from prosecution under paragraph (2)
4 of subdivision (h) which incidentally violates paragraph (2), (4),
5 or (7) of subdivision (c) shall be prosecuted under those paragraphs.

6 (j) For purposes of bringing a civil or a criminal action under
7 this section, a person who causes, by any means, the access of a
8 computer, computer system, or computer network in one
9 jurisdiction from another jurisdiction is deemed to have personally
10 accessed the computer, computer system, or computer network in
11 each jurisdiction.

12 (k) In determining the terms and conditions applicable to a
13 person convicted of a violation of this section the court shall
14 consider the following:

15 (1) The court shall consider prohibitions on access to and use
16 of computers.

17 (2) Except as otherwise required by law, the court shall consider
18 alternate sentencing, including community service, if the defendant
19 shows remorse and recognition of the wrongdoing, and an
20 inclination not to repeat the offense.