

By Senator Posey

24-163-05

1                                   A bill to be entitled

2           An act relating to Internet computer fraud;

3           providing legislative intent; defining terms;

4           prohibiting a person or a business entity from

5           using the Internet to solicit, request, or take

6           any action to induce a computer user to provide

7           personal identification information by

8           fraudulently representing that the person or

9           business is an on-line business; providing an

10          exception; prohibiting a business entity or

11          person who is not the authorized user of a

12          computer from committing certain specified

13          deceptive acts or practices that involve the

14          computer; prohibiting a person or business

15          entity from collecting certain information

16          without notice to and the consent of the

17          authorized user of the computer; providing that

18          a violation is a deceptive and unfair trade

19          practice under part II of ch. 501, F.S.;

20          authorizing a computer user to file a civil

21          action for violations of the act; providing

22          that a civil action may be filed regardless of

23          whether there is any criminal prosecution;

24          providing an effective date.

25

26 Be It Enacted by the Legislature of the State of Florida:

27

28           Section 1. Internet computer fraud.--

29           (1) LEGISLATIVE INTENT.--The Legislature finds that

30 the increasing use of fraudulent and deceptive practices

31 involving the worldwide web is a growing epidemic that

1 endangers the privacy of persons who use the Internet in the  
2 this state and adversely affects the ability of persons in  
3 this state to use their own computers and adversely affects  
4 communication, education, and commerce for persons in this  
5 state.

6 (2) DEFINITIONS.--As used in this section, the term:

7 (a) "Authorized user" or "user" means a person who  
8 owns or leases a computer or who uses a computer when  
9 authorized by its owner or lessee. The term does not include a  
10 person who has obtained authorization to use the computer  
11 solely through an end-user license agreement.

12 (b) "Business entity" means a for-profit or  
13 not-for-profit corporation, partnership, limited partnership,  
14 proprietorship, firm, enterprise, franchise, association, or  
15 trust or a self-employed individual, whether fictitiously  
16 named or not, doing business in this state, and includes a  
17 contractor or subcontractor of such a business entity.

18 (c) "Computer" means an internally programmed,  
19 automatic device that performs data processing.

20 (d) "Computer program" or "computer software" means a  
21 set of instructions or statements and related data which, when  
22 executed in actual or modified form, cause a computer,  
23 computer system, or computer network to perform specified  
24 functions.

25 (e) "Computer user" means a person in this state who  
26 uses a computer that is connected to the Internet.

27 (f) "Computer virus" means a computer program that is  
28 designed to replicate itself or affect another program or file  
29 in a computer by attaching a copy of the program or other set  
30 of instructions to one or more computer programs or files  
31 without the consent of the owner or lawful user. The term

1 includes, but is not limited to, programs that are designed to  
2 contaminate other computer programs; compromise computer  
3 security; consume computer resources; modify, destroy, record,  
4 or transmit data; or disrupt the normal operation of the  
5 computer, computer system, or computer network. The term also  
6 includes, but is not limited to, programs that are designed to  
7 use a computer without the knowledge and consent of an  
8 authorized user and to send large quantities of data to a  
9 targeted computer network without the consent of the network  
10 for the purpose of degrading the targeted computer's or  
11 network's performance or for the purpose of denying access  
12 through the network to the targeted computer or network.

13 (g) "Electronic mail message" means an electronic  
14 message or computer file that is transmitted between two or  
15 more telecommunications devices; computers; computer networks,  
16 regardless of whether the network is a local, regional, or  
17 global network; or electronic devices capable of receiving  
18 electronic messages, regardless of whether the message is  
19 converted to hard copy format after receipt, viewed upon  
20 transmission, or stored for later retrieval.

21 (h) "Internet" means the global information system  
22 that is logically linked together by a globally unique address  
23 space based on the Internet Protocol (IP), or its subsequent  
24 extensions; that is able to support communications using the  
25 Transmission Control Protocol/Internet Protocol (TCP/IP)  
26 suite, or its subsequent extensions, or other IP-compatible  
27 protocols; and that provides, uses, or makes accessible,  
28 either publicly or privately, high-level services layered on  
29 the communications and related infrastructure described in  
30 this section.

31

1           (i) "Personal identification information" means any  
2 name or number that may be used, alone or in conjunction with  
3 any other information, to identify a specific individual,  
4 including:  
5           1. A name, postal or e-mail address, social security  
6 number, date of birth, driver's license or identification  
7 number issued by a state or the Federal Government, telephone  
8 number, mother's maiden name, alien registration number,  
9 government passport number, employer or taxpayer  
10 identification number, Medicaid or food-stamp account number,  
11 bank-account number, credit-card or debit-card number, or  
12 personal-identification number or code assigned to the holder  
13 of a debit card by its issuer to permit authorized electronic  
14 use of the card;  
15           2. Unique biometric data, such as a fingerprint, voice  
16 print, retina or iris image, or other unique physical  
17 representation;  
18           3. A unique electronic identification number, address,  
19 password, or routing code;  
20           4. Medical records;  
21           5. Telecommunication identifying information or an  
22 access device;  
23           6. Account balances;  
24           7. Overdraft history;  
25           8. Payment history;  
26           9. A history of web sites visited;  
27           10. A record of a purchase or purchases; or  
28           11. Any other number or information that can be used  
29 to access an individual's financial resources.  
30           (j) "Transmit" means to transfer, send, or make  
31 available computer programs or software, or any component of

1 computer software, via the Internet or any other medium,  
2 including local area networks of computers, any other nonwire  
3 transmission, or any disk or other data storage device.

4 (k) "Web page" means a location with respect to the  
5 worldwide web which has a single uniform resource locator or  
6 other single location with respect to the Internet.

7 (3) PROHIBITION AGAINST PHISHING OR FRAUD-BASED WEB  
8 SITES.--A person or a business entity may not, by means of a  
9 web page, electronic mail message, or other use of the  
10 Internet, solicit, request, or take any action to induce a  
11 computer user to provide personal identification information  
12 by representing that the person or business entity soliciting  
13 or requesting the information, either directly or by  
14 implication, is an on-line business, unless the person or  
15 entity has the authority and approval of the on-line business  
16 to make that representation.

17 (4) PROTECTION AGAINST DECEPTIVE ACTS OR PRACTICES  
18 RELATING TO SPYWARE.--A business entity or person who is not  
19 the authorized user of a computer may not engage in deceptive  
20 acts or practices that involve any of the following conduct  
21 with respect to the computer:

22 (a) Taking control of the computer by:

23 1. Using the computer to send unsolicited information  
24 or material from the computer to others;

25 2. Diverting the Internet browser of the computer or  
26 any similar program of the computer used to access and  
27 navigate the Internet:

28 a. Away from the site the authorized user intended to  
29 view to one or more other web pages, such that the user is  
30 prevented from viewing the content at the intended web page;  
31 and

1           b. Without permission of the authorized user of the  
2 computer, unless the diverting is otherwise authorized;

3           3. Accessing or using the modem or Internet connection  
4 or service for the computer and thereby causing damage to the  
5 computer or causing the authorized user to incur unanticipated  
6 financial charges;

7           4. Using the computer as part of an activity performed  
8 by a group of computers to cause damage to another computer;  
9 or

10           5. Delivering advertisements that a user of the  
11 computer cannot close without turning off the computer or  
12 closing all sessions of the Internet browser for the computer.

13           (b) Modifying settings related to use of the computer  
14 or to the computer's access to or use of the Internet by  
15 altering:

16           1. The web page that appears when the authorized user  
17 launches an Internet browser or similar program used to access  
18 and navigate the Internet;

19           2. The default provider used to access or search the  
20 Internet, or other existing Internet connections settings;

21           3. A list of bookmarks used by the computer to access  
22 web pages; or

23           4. Security or other settings of the computer which  
24 protect information about the authorized user for the purposes  
25 of causing damage or harm to the computer or its owner or  
26 user.

27           (c) Collecting personal identification information  
28 through the use of a keystroke logging function.

29           (d) Inducing the authorized user to install a computer  
30 software component onto the computer, or preventing reasonable  
31

1 efforts to block the installation or execution of, or to  
2 disable, a computer software component by:

3 1. Presenting the authorized user with an option to  
4 decline installation of a software component such that, when  
5 the option is selected by the owner or authorized user, the  
6 installation nevertheless proceeds; or

7 2. Causing a computer software component that the  
8 authorized user has properly removed or disabled to  
9 automatically reinstall or reactivate on the computer.

10 (e) Misrepresenting that installing a separate  
11 software component or providing log-in and password  
12 information is necessary for security or privacy reasons, or  
13 that installing a separate software component is necessary to  
14 open, view, or play a particular type of content.

15 (f) Inducing the authorized user to install or execute  
16 computer software by misrepresenting the identity or authority  
17 of the person or business entity providing the computer  
18 software to the user.

19 (g) Inducing the authorized user to provide personal  
20 identification, password, or account information to another  
21 person:

22 1. By misrepresenting the identify of the person  
23 seeking the information; or

24 2. Without the authority of that user's intended  
25 recipient of the information.

26 (h) Removing, disabling, or rendering inoperative a  
27 security, anti-spyware, or anti-virus technology installed on  
28 the computer.

29 (i) Installing or executing on the computer one or  
30 more additional computer software components with the intent  
31

1 of causing a person to use the components in a way that  
2 violates any other provision of this section.

3 (5) PROHIBITION OF COLLECTION OF CERTAIN INFORMATION  
4 WITHOUT NOTICE AND CONSENT.--

5 (a) Except as provided in paragraph (e), a business  
6 entity or person may not:

7 1. Transmit to a computer, which is not owned by that  
8 business entity or person and for which that business entity  
9 or person is not an authorized user, any  
10 information-collection program, unless the  
11 information-collection program provides notice in accordance  
12 with paragraph (c) before execution of any of the  
13 information-collection functions of the program; or

14 2. Execute any information-collection program  
15 installed on the computer unless before execution of any of  
16 the information-collection functions of the program the  
17 authorized user of the computer has consented to the execution  
18 under notice in accordance with paragraph (c).

19 (b) For purposes of this subsection, the term  
20 "information-collection program" means computer software that:

21 1. Collects personal identifying information and sends  
22 that information to a person other than the authorized user of  
23 the computer or uses that information to deliver advertising  
24 to, or display advertising on, the computer; or

25 2. Collects information regarding the web pages  
26 accessed using the computer and uses that information to  
27 deliver advertising to, or display advertising on, the  
28 computer.

29 (c) The notice required by this subsection with  
30 respect to an information-collection program must be clear and  
31



1 conspicuous, must be given in plain language, and must satisfy  
2 all of the following:  
3       1. The notice must be clearly distinguishable from any  
4 other information visually presented contemporaneously on the  
5 protected computer.  
6       2. The notice must contain one of the following  
7 statements, as applicable, or a substantially similar  
8 statement:  
9       a. With respect to an information-collection program  
10 described in subparagraph (b)1.: "This program will collect  
11 and transmit information about you. Do you accept?"  
12       b. With respect to an information-collection program  
13 described in subparagraph (b)2.: "This program will collect  
14 information about web pages you access and will use that  
15 information to display advertising on your computer. Do you  
16 accept?"  
17       c. With respect to an information-collection program  
18 that performs the actions described in both subparagraphs  
19 (b)1. and 2.: "This program will collect and transmit  
20 information about you and your computer use and will collect  
21 information about web pages you access and will use that  
22 information to display advertising on your computer. Do you  
23 accept?"  
24       3. The notice must allow the user to:  
25       a. Grant or deny consent by selecting an option to  
26 grant or deny consent; and  
27       b. Abandon or cancel the transmission or execution  
28 referred to in paragraph (a) without granting or denying  
29 consent.  
30  
31

1           4. The notice must allow the user to select to display  
2 on the computer, before granting or denying consent using the  
3 option required under subparagraph 3., a clear description of:

4           a. The types of information to be collected and sent,  
5 if any, by the information-collection program;

6           b. The purpose for which the information is to be  
7 collected and sent; and

8           c. In the case of an information-collection program  
9 that first executes any of the information-collection  
10 functions of the program upon the next execution of other  
11 computer software, the identity of that other computer  
12 software.

13           5. The notice must provide for concurrent display of  
14 the information required under subparagraphs 2. and 3. and the  
15 option required under subparagraph 4. until the user:

16           a. Grants or denies consent using the option required  
17 under sub-subparagraph 3.a.;

18           b. Abandons or cancels the transmission or execution  
19 pursuant to sub-subparagraph 3.b.; or

20           c. Selects the option required under subparagraph 4.

21           (d) If an authorized user has granted consent to the  
22 execution of an information-collection program under a notice  
23 given in compliance with this subsection, no subsequent notice  
24 is required. However, the person who transmitted the program  
25 shall provide another notice in accordance with this  
26 subsection and obtain consent before the program may be used  
27 to collect or send information of a type or for a purpose that  
28 is materially different from, and outside the scope of, the  
29 type or purpose set forth in any previous notice.

30           (6) PENALTIES.--A business entity or person who  
31 violates this section commits a deceptive and unfair trade

1 practice in violation of part II of chapter 501, Florida  
2 Statutes, and is subject to the penalties and remedies  
3 provided by that chapter.

4 (7) CIVIL REMEDIES.--

5 (a) A computer user, including an individual who is  
6 engaged in the business of providing Internet access service  
7 or who owns a web page or trademark, whose property or person  
8 is injured as a result of a violation of this section may:

9 1. Institute a civil action to enjoin and restrain  
10 future violations of this section and to recover actual  
11 losses, lost wages, attorney's fees, and other costs incurred  
12 by the computer user or resulting from the misappropriation of  
13 the personal identification information of the computer user.

14 2. Bring a civil suit for damages in an amount of up  
15 to \$5,000 for each incident, or three times the amount of  
16 actual damages, whichever amount is greater. The court, in an  
17 action brought under this subparagraph, may award reasonable  
18 attorney's fees to the prevailing party.

19 (b) The venue for a civil action brought under this  
20 subsection shall be the county in which the plaintiff resides  
21 or in any county in which any part of the alleged violation of  
22 this section took place, regardless of whether the defendant  
23 was ever actually present in that county. A civil action filed  
24 under this subsection must be brought within 5 years after the  
25 violation occurred.

26 (c) A civil action may be filed under this subsection  
27 regardless of whether there is any criminal prosecution for  
28 the acts that are the subject of the civil action. The rights  
29 and remedies provided by this subsection are in addition to  
30 any other rights and remedies provided by law.

31 Section 2. This act shall take effect July 1, 2005.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31

\*\*\*\*\*

SENATE SUMMARY

Prohibits a person or a business entity from using the Internet to solicit, request, or take any action to induce a computer user to provide personal identification information by fraudulently representing that the person or business is an on-line business. Provides an exception. Prohibits a business entity or person who is not the authorized user of a computer from engaging in certain specified deceptive acts or practices that involve a computer. Prohibits a person or business entity from collecting certain information without giving notice and obtaining the consent of the authorized user of the computer. Provides that a business entity or person who violates the act commits a deceptive and unfair trade practice in violation of part II of ch. 501, F.S. Authorizes a computer user to file a civil action for violations of the act.