E-Commerce Integrity

This Act prohibits certain Internet-related conduct, including phishing, pharming, spyware, and cybersquatting. For example, the legislation prohibits a person from using electronic communications to facilitate certain types of fraud and injury and it allows for removing domain names and online content by an Internet registrar or Internet Service Provider under certain circumstances. The legislation also prohibits political subdivisions of the state from enacting conflicting laws.

Submitted as:
Utah
SB 26 (Enrolled Copy)
Status: Enacted into law in 2010.

Suggested State Legislation

(Title, enacting clause, etc.)

Section 1. [Short Title.] This Act shall be cited as “The E-Commerce Integrity Act.”

Section 2. [Definitions.] As used in this Act:
(1) (a) “Cause to be copied” means to distribute or transfer computer software, or any component of computer software.
(b) “Cause to be copied” does not include providing:
(I) transmission, routing, intermediate temporary storage, or caching of software;
(II) a storage or hosting medium, such as a compact disk, website, or computer server through which the software was distributed by a third party; or
(III) an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which the user of the computer located the software.
(2) (a) “Computer software” means a sequence of instructions written in any programming language that is executed on a computer.
(b) “Computer software” does not include a data component of a webpage that is not executable independently of the webpage.
(3) “Computer virus” means a computer program or other set of instructions that is designed to degrade the performance of or disable a computer or computer network and is designed to have the ability to replicate itself on another computer or computer network without the authorization of the owner of the other computer or computer network.
(4) “Damage” means any significant impairment to the performance of a computer or integrity or availability of data, software, a system, or information.
(5) “Execute,” when used with respect to computer software, means the performance of the functions or the carrying out of the instructions of the computer software.
(6) “False pretenses” means the representation of a fact or circumstance that is not true and is calculated to mislead.
(7) (a) “Identifying information” means any information that can be used to access a person’s financial accounts or to obtain goods and services, including the person’s:
(I) address;
(II) birth date;
(III) Social Security number;
(IV) driver license number;
(V) non-driver governmental identification number;
(VI) telephone number;
(VII) bank account number;
(VIII) student identification number;
(IX) credit or debit card number;
(X) personal identification number;
(XI) unique biometric data;
(XII) employee or payroll number;
(XIII) automated or electronic signature;
(XIV) computer image file;
(XV) photograph; or
(XVI) computer screen name or password.

(b) “Identifying information” does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

(8) “Intentionally deceptive” means any of the following:
(a) an intentionally and materially false or fraudulent statement;
(b) a statement or description that intentionally omits or misrepresents material information in order to deceive an owner or operator of a computer; or
(c) an intentional and material failure to provide a notice to an owner or operator concerning the installation or execution of computer software, for the purpose of deceiving the owner or operator.

(9) “Internet” means the global information system that is logically linked together by a globally unique address space based on the Internet protocol (IP), or its subsequent extensions, and that is able to support communications using the transmission control protocol/Internet protocol (TCP/IP) suite, or its subsequent extensions, or other IP-compatible protocols, and that provides, uses, or makes accessible, either publicly or privately, high-level services layered on communications and related infrastructure.

(10) “Internet service provider” means:
(a) an Internet service provider, as defined in [insert citation] or a hosting company as defined in [insert citation.]

(11) “Message” means a graphical or text communication presented to an authorized user of a computer.

(12) (a) “Owner or operator” means the owner or lessee of a computer, or a person using a computer with the owner’s or lessee’s authorization.
(b) “Owner or operator” does not include a person who owned a computer before the first retail sale of the computer.

(13) “Person” means any individual, partnership, corporation, limited liability company, or other organization, or any combination thereof.

(14) “Personally identifiable information” means any of the following information if it allows the entity holding the information to identify the owner or operator of a computer:
(a) the first name or first initial in combination with the last name and a home or other physical address including street name;
(b) a personal identification code in conjunction with a password required to access an identified account, other than a password, personal identification number, or other identification number transmitted by an authorized user to the issuer of the account or its agent;
(c) a Social Security number, tax identification number, driver license number, passport number, or any other government-issued identification number; or

(d) an account balance, overdraft history, or payment history that personally identifies an owner or operator of a computer.

(15) “Webpage” means a location that has a single uniform resource locator (URL) with respect to the World Wide Web or another location that can be accessed on the Internet.

Section 3. [Application.] This Act applies to conduct involving a computer, software, or an advertisement located in, sent to, or displayed in this state.

Section 4. [Phishing and Pharming.]

(A) A person is guilty of phishing if, with intent to defraud or injure an individual, or with knowledge that the person is facilitating a fraud or injury to be perpetrated by another, the person makes a communication under false pretenses purporting to be by or on behalf of a legitimate business, without the authority or approval of the legitimate business and the person uses the communication to induce, request, or solicit another person to provide identifying information or property.

(B) A person is guilty of pharming if, with intent to defraud or injure another, or with knowledge that the person is facilitating a fraud or injury to be perpetrated by another, the person:

(1) creates or operates a webpage that represents itself as belonging to or being associated with a legitimate business, without the authority or approval of the legitimate business, if that webpage may induce any user of the Internet to provide identifying information or property; or

(2) alters a setting on a user’s computer or similar device or software program through which the user may search the Internet, causing any user of the Internet to view a communication that represents itself as belonging to or being associated with a legitimate business, if the message has been created or is operated without the authority or approval of the legitimate business and induces, requests, or solicits any user of the Internet to provide identifying information or property.

(C) A civil action against a person who violates any provision of this Section may be filed by an Internet service provider that is adversely affected by the violation; an owner of a webpage, computer server, or a trademark that is used without authorization in the violation; or the [attorney general].

(D) A person permitted to bring a civil action under Subsection (C) may obtain either actual damages for a violation of this Section or a civil penalty not to exceed [$150,000] per violation.

(E) A violation of this Section by a state-chartered or licensed financial institution is enforceable exclusively by the financial institution’s primary state regulator.

(F) This Section applies to the discovery of a phishing or pharming incident that occurs on or after [insert date].

(G) This Section does not apply to a telecommunications provider’s or Internet service provider’s good faith transmission or routing of, or intermediate temporary storing or caching of, identifying information.

(H) If an Internet registrar or Internet service provider believes in good faith that an Internet domain name controlled or operated by the Internet registrar or Internet service provider, or content residing on an Internet website or other online location controlled or operated by the Internet registrar or Internet service provider, is used to engage in a violation of this Section, the Internet registrar or Internet service provider is not liable under any provision of the laws of this
state or of any political subdivision of the state for removing or disabling access to the Internet
domain name or other content.

(I) The conduct prohibited by this Section is of statewide concern, and this Section’s
provisions supersede and preempt any provision of law of a political subdivision of the state.

Section 5. [Spyware: Prohibitions on The Use of Computer Software.]
(A) A person who is not an owner or operator of a computer may not cause computer
software to be copied on the computer knowingly, with conscious avoidance of actual
knowledge, or willfully, if the software is used to:

(1) modify, through intentionally deceptive means, settings of a computer
controlling:

(a) the webpage that appears when an owner or operator launches an
Internet browser or similar computer software used to access and navigate the Internet;
(b) the default provider or web proxy that an owner or operator uses to
access or search the Internet; or
(c) an owner’s or an operator’s list of bookmarks used to access webpages;

(2) collect, through intentionally deceptive means, personally identifiable
information:

(a) through the use of a keystroke-logging function that records all or
substantially all keystrokes made by an owner or operator of a computer and transfers that
information from the computer to another person;
(b) in a manner that correlates personally identifiable information with
data concerning all or substantially all of the webpages visited by an owner or operator, other
than webpages operated by the person providing the software, if the computer software was
installed in a manner designed to conceal from all authorized users of the computer the fact that
the software is being installed; or
(c) by extracting from the hard drive of an owner’s or an operator’s
computer, an owner’s or an operator’s Social Security number, tax identification number, driver
license number, passport number, any other government-issued identification number, an
account balance, or overdraft history for a purpose unrelated to any of the purposes of the
software or service described to an authorized user;

(3) prevent, through intentionally deceptive means, an owner’s or an operator’s
reasonable efforts to block or disable the installation or execution of computer software by
causeing computer software that the owner or operator has properly removed or disabled to
automatically reinstall or reactivate on the computer without the authorization of an authorized
user;

(4) intentionally misrepresent that computer software will be uninstalled or
disabled by an owner’s or an operator’s action;

(5) through intentionally deceptive means, remove, disable, or render inoperative
security, antispyware, or antivirus computer software installed on an owner’s or an operator’s
computer;

(6) enable use of an owner’s or an operator’s computer to:

(a) access or use a modem or Internet service for the purpose of causing
damage to an owner’s or an operator’s computer or causing an owner or operator, or a third party
affected by that conduct, to incur financial charges for a service that the owner or operator did
not authorize;

(b) open multiple, sequential, stand-alone messages in an owner’s or an
operator’s computer without the authorization of an owner or operator and with knowledge that a
reasonable computer user could not close the messages without turning off the computer or
closing the software application in which the messages appear, unless the communication originated from the computer’s operating system, a software application the user activated, or a service provider that the user chose to use, or was presented for any of the purposes described in Section 6 of this Act; or
(c) transmit or relay commercial electronic mail or a computer virus from the computer, if the transmission or relay is initiated by a person other than the authorized user without the authorization of an authorized user;

(7) modify, without the authorization of an owner or operator, any of the following settings related the computer’s access to, or use of, the Internet:
(a) settings that protect information about an owner or operator for the purpose of taking personally identifiable information of the owner or operator;
(b) security settings, for the purpose of causing damage to a computer; or
(c) settings that protect the computer from the uses identified in Subsection (A)(6); or

(8) prevent, without the authorization of an owner or operator, an owner’s or an operator’s reasonable efforts to block the installation of, or to disable, computer software by:
(a) presenting the owner or operator with an option to decline installation of computer software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds;
(b) falsely representing that computer software has been disabled;
(c) requiring in an intentionally deceptive manner the user to access the Internet to remove the software with knowledge or reckless disregard of the fact that the software frequently operates in a manner that prevents the user from accessing the Internet;
(d) changing the name, location, or other designation information of the software for the purpose of preventing an authorized user from locating the software to remove it;
(e) using randomized or intentionally deceptive filenames, directory folders, formats, or registry entries for the purpose of avoiding detection and removal of the software by an authorized user;
(f) causing the installation of software in a particular computer directory or in computer memory for the purpose of evading an authorized user’s attempt to remove the software from the computer; or
(g) requiring, without the authority of the owner of the computer, that an authorized user obtain a special code or download software from a third party to uninstall the software.

(B) (1) The attorney general, an Internet service provider, or a software company that expends resources in good faith assisting authorized users harmed by a violation of this Section or a trademark owner whose mark is used to deceive authorized users in violation of this Section, may bring a civil action against a person who violates this Section to recover actual damages and liquidated damages of at least [$1,000] per violation of this Section not to exceed [$1,000,000] for a pattern or practice of violations and attorney fees and costs.

(2) The court may increase a damage award to an amount equal to not more than [three] times the amount otherwise recoverable under Subsection (1) if the court determines that the defendant committed the violation willfully and knowingly.

(3) The court may reduce liquidated damages recoverable under Subsection (1) to a minimum of [$100, not to exceed $100,000] for each violation, if the court finds that the defendant established and implemented practices and procedures reasonably designed to prevent a violation of this Section.
(4) In the case of a violation of Subsection (A)(6) that causes a telecommunications carrier or provider of voice over Internet protocol service to incur costs for the origination, transport, or termination of a call triggered using the modem or Internet-capable device of a customer of the telecommunications carrier or provider of voice over Internet protocol as a result of the violation, the telecommunications carrier or provider of voice over Internet protocol may bring a civil action against the violator:

(a) to recover the charges the telecommunications carrier or provider of voice over Internet protocol is required to pay to another carrier or to an information service provider as a result of the violation, including charges for the origination, transport, or termination of the call;

(b) to recover the costs of handling customer inquiries or complaints with respect to amounts billed for the calls;

(c) to recover reasonable attorney fees and costs; and

(d) for injunctive relief.

(5) For purposes of a civil action under Subsections (1), (2), and (3), a single action or conduct that violates more than one provision of this Section, shall be considered as multiple violations based on the number of provisions violated.

Section 6. [Other Prohibited Conduct.] A person who is not an owner or operator of a computer may not, with regard to the computer induce an owner or operator to install a computer software component onto the owner’s or the operator’s computer by intentionally misrepresenting that installing the computer software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content or use intentionally deceptive means to cause the execution of a computer software component with the intent of causing the computer to use the computer software component in a manner that violates any other provision of this [Act].

Section 7. [Exceptions.] Sections 5 and 6 of this Act do not apply to the monitoring of, or interaction with, an owner’s or an operator’s Internet or other network connection, service, or computer, by a telecommunications carrier, cable operator, computer hardware or software provider, or provider of information service or interactive computer service for network or computer security purposes, diagnostics, technical support, maintenance, repair, network management, authorized updates of computer software or system firmware, authorized remote system management, or detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software, including scanning for and removing computer software prescribed under [insert citation].

Section 8. [Cybersquatting.] (A) A person is liable in a civil action by the owner of a mark, including a personal name, which is a mark for purposes of this Section, if, without regard to the goods or services of the person or the mark’s owner, the person has a bad faith intent to profit from the mark, including a personal name and for any length of time registers, acquires, traffics in, or uses a domain name in, or belonging to any person in, this state that:

(1) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to the mark;

(2) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of the mark; or

(3) is a trademark, word, or name protected by reason of 18 U.S.C. Sec. 706 or 348 U.S.C. Sec. 220506.
(B) In determining whether a person has a bad faith intent described in Subsection (A), a court may consider all relevant factors, including:

(1) the trademark or other intellectual property rights of the person, if any, in the domain name;
(2) the extent to which the domain name consists of the legal name of the person or a name that is otherwise commonly used to identify that person;
(3) the person’s prior use, if any, of the domain name in connection with the bona fide offering of any goods or services;
(4) the person’s bona fide noncommercial or fair use of the mark in a site accessible under the domain name;
(5) the person’s intent to divert consumers from the mark owner’s online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site;
(6) the person’s offer to transfer, sell, or otherwise assign, or solicitation of the purchase, transfer, or assignment of the domain name to the mark owner or any third party for financial gain without having used, or having an intent to use, the domain name in the bona fide offering of any goods or services, or the person’s prior conduct indicating a pattern of such conduct;
(7) the person’s provision of material and misleading false contact information when applying for the registration of the domain name, the person’s intentional failure to maintain accurate contact information, or the person’s prior conduct indicating a pattern of such conduct;
(8) the person’s registration or acquisition of multiple domain names that the person knows are identical or confusingly similar to another’s mark that is distinctive at the time of registration of the domain names, or is dilutive of another’s famous mark that is famous at the time of registration of the domain names, without regard to the goods or services of the person or the mark owner; and
(9) the extent to which the mark incorporated in the person’s domain name registration is or is not distinctive and famous.

(C) Bad faith intent described in Subsection (A) may not be found in any case in which the court determines that the person believed and had reasonable grounds to believe that the use of the domain name was a fair use or otherwise lawful.

(D) In a civil action involving the registration, trafficking, or use of a domain name under this section, a court may order the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

(E) A person is liable for using a domain name under Subsection (A) only if that person is the domain name registrant or that registrant’s authorized licensee, affiliate, domain name registrar, domain name registry, or other domain name registration authority that knowingly assists a violation of this Act by the registrant.

(F) A person may not be held liable under this Section absent a showing of bad faith intent to profit from the registration or maintenance of the domain name.

(G) For purposes of this section, a “showing of bad faith intent to profit” shall be interpreted in the same manner as under 15 U.S.C. Sec. 1114(2)(D)(iii).

(H) As used in this Section, the term “traffics in” refers to transactions that include sales, purchases, loans, pledges, licenses, exchanges of currency, and any other transfer for consideration or receipt in exchange for consideration.
The owner of a mark registered with the U.S. Patent and Trademark Office or under this Act may file an in rem civil action against a domain name in the district court if the owner is located in the state and if:

(1) the domain name violates any right of the owner of a mark registered in the Patent and Trademark Office or registered under this Act; and

(2) the court finds that the owner:
   (a) is not able to obtain personal jurisdiction over a person who would be a defendant in a civil action under Subsection (A); or
   (b) through due diligence was not able to find a person who would be a defendant in a civil action under Subsection (A) by:
      (I) sending a notice of the alleged violation and intent to proceed under this Subsection to the registrant of the domain name at the postal and e-mail address provided by the registrant to the registrar; and
      (III) publishing notice of the action as the court may direct promptly after filing the action.

(J) Completion of the actions required by Subsection (I) (2) (b) constitutes service of process.

(K) In an in rem action under this Subsection (I), a domain name is considered to be located in the judicial district in which the domain name registrar, registry, or other domain name authority that registered or assigned the domain name is located or documents sufficient to establish control and authority regarding the disposition of the registration and use of the domain name are deposited with the court.

(L) The remedies in an in rem action under this Subsection (I) are limited to a court order for the forfeiture or cancellation of the domain name or the transfer of the domain name to the owner of the mark.

(M) Upon receipt of written notification of a filed, stamped copy of a complaint filed by the owner of a mark in the district court under this Subsection (I), the domain name registrar, domain name registry, or other domain name authority shall expeditiously deposit with the court documents sufficient to establish the court’s control and authority regarding the disposition of the registration and use of the domain name to the court and not transfer, suspend, or otherwise modify the domain name during the pendency of the action, except upon order of the court.

(N) The domain name registrar or registry or other domain name authority is not liable for injunctive or monetary relief under this section, except in the case of bad faith or reckless disregard, which includes a willful failure to comply with a court order.

(O) The civil actions and remedies established by Subsection (A) and the in rem action established in Subsection (I) do not preclude any other applicable civil action or remedy.

(P) The in rem jurisdiction established under Subsection (I) does not preclude any other jurisdiction, whether in rem or personal.

Section 9. [Infringement.]

(A) Subject to [insert citation] and Subsection (B), any person is liable in a civil action brought by the registrant for any and all of the remedies provided in [insert citation], if that person:

(1) uses a reproduction, counterfeit, copy, or colorable imitation of a mark registered under this Act without the consent of the registrant and in connection with the sale, distribution, offering for sale, or advertising of any goods or services on or in connection with which that use is likely to cause confusion, mistake, or to deceive as to the source of origin, nature, or quality of those goods or services; or
(2) reproduces, counterfeits, copies, or colorably imitates any mark and applies the reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints, packages, wrappers, receptacles, or advertisements intended to be used upon or in connection with the sale or other distribution in this state of goods or services.

(B) Under Subsection (A)(1), the registrant is not entitled to recover profits or damages unless the act described in Subsection (A)(1) has been committed with the intent to cause confusion or mistake or to deceive.

(C) In a civil action for a violation of Section 8 of this Act, the plaintiff may recover court costs and reasonable attorney fees and the plaintiff may elect, at any time before final judgment is entered by the district court, to recover, instead of actual damages and profits, an award of statutory damages in the amount of not less than [$1,000] and not more than [$100,000] per domain name, as the court considers just. Statutory damages awarded under this Subsection are presumed to be [$100,000] per domain name if there is a pattern and practice of infringements committed willfully for commercial gain.

Section 10. [Severability.] [Insert severability clause.]

Section 11. [Repealer.] [Insert repealer clause.]

Section 12. [Effective Date.] [Insert effective date.]