

1 HB400
2 136824-1
3 By Representative DeMarco
4 RFD: Judiciary
5 First Read: 23-FEB-12

2
3
4
5
6
7
8 SYNOPSIS: Existing law makes it a crime for a person
9 to knowingly and willfully without authorization
10 access or modify certain information or programs on
11 a computer or in the computer system or network of
12 another.

13 This bill would repeal the existing computer
14 crime act and replace it with the Alabama Digital
15 Crime Act.

16 This bill would make computer tampering a
17 crime and would describe what acts constitute this
18 crime.

19 This bill would make encoded data fraud a
20 crime and would describe what acts constitute this
21 crime.

22 This bill would make phishing a crime and
23 would describe what acts constitute this crime.

24 This bill would make electronic harassment
25 and cyberstalking crimes and would describe what
26 acts constitute these crimes.

1 This bill would establish jurisdiction to
2 prosecute certain computer crimes and jurisdiction
3 of records related to the investigation of certain
4 computer crimes.

5 This bill would provide for forfeiture of a
6 computer or computer system owned by a defendant
7 and used in the commission of a crime.

8 Amendment 621 of the Constitution of Alabama
9 of 1901, now appearing as Section 111.05 of the
10 Official Recompilation of the Constitution of
11 Alabama of 1901, as amended, prohibits a general
12 law whose purpose or effect would be to require a
13 new or increased expenditure of local funds from
14 becoming effective with regard to a local
15 governmental entity without enactment by a 2/3 vote
16 unless: it comes within one of a number of
17 specified exceptions; it is approved by the
18 affected entity; or the Legislature appropriates
19 funds, or provides a local source of revenue, to
20 the entity for the purpose.

21 The purpose or effect of this bill would be
22 to require a new or increased expenditure of local
23 funds within the meaning of the amendment. However,
24 the bill does not require approval of a local
25 governmental entity or enactment by a 2/3 vote to
26 become effective because it comes within one of the
27 specified exceptions contained in the amendment.

1
2 A BILL
3 TO BE ENTITLED
4 AN ACT
5

6 To provide for the crimes of computer tampering,
7 encoded data fraud, phishing, electronic harassment, and
8 cyberstalking; to provide for jurisdiction in the
9 investigation and prosecution of certain computer crimes; to
10 provide for forfeiture of certain computers used in a crime;
11 to repeal Sections 13A-8-100, 13A-8-101, 13A-8-102, and
12 13A-8-103, Code of Alabama 1975; and in connection therewith
13 would have as its purpose or effect the requirement of a new
14 or increased expenditure of local funds within the meaning of
15 Amendment 621 of the Constitution of Alabama of 1901, now
16 appearing as Section 111.05 of the Official Recompilation of
17 the Constitution of Alabama of 1901, as amended.

18 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

19 Section 1. This act may be cited as The Alabama
20 Digital Crime Act.

21 Section 2. As used in this act, the following terms
22 shall have the following meanings:

23 (1) ACCESS. To gain entry to, instruct, communicate
24 with, store data in, retrieve or intercept data from, alter
25 data or computer software in, or otherwise make use of any
26 resource of a computer, computer system, or computer network.

1 (2) COMPUTER. An electronic, magnetic, optical,
2 electrochemical, or other high speed data processing device or
3 system that performs logical, arithmetic, or memory functions
4 by the manipulations of electronic or magnetic impulses and
5 includes all input, output, processing, storage, or
6 communication facilities that are connected or related to the
7 device.

8 (3) COMPUTER NETWORK. The interconnection of two or
9 more computers or computer systems that transmit data over
10 communication circuits connecting them.

11 (4) COMPUTER PROGRAM. An ordered set of data
12 representing coded instructions or statements that when
13 executed by a computer cause the computer to process data or
14 perform specific functions.

15 (5) COMPUTER SECURITY SYSTEM. The design,
16 procedures, or other measures that the person responsible for
17 the operation and use of a computer employs to restrict the
18 use of the computer to particular persons or uses or that the
19 owner or licensee of data stored or maintained by a computer
20 in which the owner or licensee is entitled to store or
21 maintain the data employs to restrict access to the data.

22 (6) COMPUTER SERVICES. The product of the use of a
23 computer, the information stored in the computer, or the
24 personnel supporting the computer, including computer time,
25 data processing, and storage functions.

26 (7) COMPUTER SOFTWARE. A set of instructions or
27 statements, and related data, that when executed in actual or

1 modified form, cause a computer, computer system, or computer
2 network to perform specific functions.

3 (8) COMPUTER SYSTEM. A set of related or
4 interconnected computer or computer network equipment, devices
5 and software.

6 (9) DATA. A representation of information,
7 knowledge, facts, concepts, or instructions, which are
8 prepared and are intended for use in a computer, computer
9 system, or computer network. Data may be in any form, in
10 storage media, or as stored in the memory of the computer or
11 in transit.

12 (10) ELECTRONIC MAIL MESSAGE. A message sent to a
13 unique destination that consists of a unique user name or
14 mailbox and a reference to an Internet domain, whether or not
15 displayed, to which such message can be sent or delivered.

16 (11) FINANCIAL INSTRUMENT. Includes, but is not
17 limited to, any check, cashier's check, draft, warrant, money
18 order, certificate of deposit, negotiable instrument, letter
19 of credit, bill of exchange, credit or debit card, transaction
20 authorization mechanism, marketable security, or any computer
21 system representation thereof.

22 (12) HARM. Partial or total alteration, damage, or
23 erasure of stored data, interruption of computer services,
24 introduction of a virus, or any other loss, disadvantage, or
25 injury that might reasonably be suffered as a result of the
26 actor's conduct.

1 (13) IDENTIFICATION DOCUMENT. Any document
2 containing data that is issued to an individual and which that
3 individual, and only that individual, uses alone or in
4 conjunction with any other information for the primary purpose
5 of establishing his or her identity or accessing his or her
6 financial information or benefits. Identification documents
7 specifically include, but are not limited to, the following:

8 a. Government issued driver's licenses or
9 identification cards.

10 b. Payment cards such as credit cards, debit cards,
11 and ATM cards.

12 c. Passports.

13 d. Health insurance or benefit cards.

14 e. Identification cards issued by educational
15 institutions.

16 f. Identification cards for employees or
17 contractors.

18 g. Benefit cards issued in conjunction with any
19 government supported aid program.

20 h. Library cards issued by any public library.

21 (14) IDENTIFYING INFORMATION. Specific details that
22 can be used to access a person's financial accounts, obtain
23 identification, or to obtain goods or services, including, but
24 not limited to:

25 a. Social Security number.

26 b. Driver's license number.

27 c. Bank account number.

- d. Credit card or debit card number.
- e. Personal identification number (PIN).
- f. Automated or electronic signature.
- g. Unique biometric data.
- h. Account password.

(15) INTEGRATED CIRCUIT CARD. Also known as a smart card or chip card, a pocket sized, plastic card with embedded integrated circuits used for data storage or special purpose processing used to validate personal identification numbers (PINs), authorize purchases, verify account balances and store personal records. When inserted into a reader, it transfers data to and from a central computer.

(16) OWNER. An owner or lessee of a computer or a computer network, or an owner, lessee, or licensee of computer data, computer programs, or computer software.

(17) PROPERTY. Includes a financial instrument, data, databases, data while in transit, computer software, computer programs, documents associated with computer systems and computer programs, or copies whether tangible or intangible.

(18) RADIO FREQUENCY IDENTIFICATION (RFID). A technology that uses radio waves to transmit data remotely from an RFID tag, through a reader, from identification documents. It is used in contactless integrated circuit cards, also known as proximity cards.

(19) RADIO FREQUENCY IDENTIFICATION (RFID) TAGS. Also known as RFID labels, the hardware for an RFID system

1 that electronically stores and processes information, and
2 receives and transmits the signal.

3 (20) REENCODER. An electronic device that places
4 encoded information from the magnetic strip, integrated
5 circuit, RFID tag of an identification document onto the
6 magnetic strip, integrated circuit, or RFID tag of a different
7 identification document.

8 (21) SCANNING DEVICE. A scanner, reader, or any
9 other electronic device that is used to access, read, scan,
10 obtain, memorize, or store, temporarily or permanently,
11 information encoded on the magnetic strip, integrated circuit,
12 or RFID tag of an identification document.

13 (22) TRAIT OR CHARACTERISTIC OF THAT PERSON.
14 Includes, but is not limited to, age, color, creed, national
15 origin, race, religion, marital status, sex, sexual
16 orientation, gender identity, ancestry, political party
17 preferences, political beliefs, socio-economic status, family
18 status, or education.

19 (23) VIRUS. Means an unwanted computer program or
20 other set of instructions inserted into a computer's memory,
21 operating system, or program that is specifically constructed
22 with the ability to replicate itself or to affect the other
23 programs or files in the computer by attaching a copy of the
24 unwanted program or other set of instructions to one or more
25 computer programs or files.

1 (24) WEB PAGE. A location that has a single uniform
2 resource locator or other single location with respect to the
3 Internet.

4 Section 3. (a) A person who acts without authority
5 or who exceeds authorization of use commits the crime of
6 computer tampering by knowingly or recklessly:

7 (1) Accessing, altering, damaging, or destroying any
8 computer, computer system, or computer network.

9 (2) Altering, damaging, deleting, or destroying
10 computer programs or data.

11 (3) Disclosing, using, controlling, or taking
12 computer programs, data, or supporting documentation residing
13 in, or existing internal or external to, a computer, computer
14 system, or network.

15 (4) Directly or indirectly introducing a computer
16 contaminator or a virus into any computer, computer system, or
17 network.

18 (5) Disrupting or causing the disruption of a
19 computer, computer system, or network services or denying or
20 causing the denial of computer or network services to any
21 authorized user of a computer, computer system, or network.

22 (6) Preventing a computer user from exiting a site,
23 computer system, or network-connected location in order to
24 compel the user's computer to continue communicating with,
25 connecting to, or displaying the content of the service, site,
26 or system.

1 (7) Obtaining any information that is required by
2 law to be kept confidential or any records that are not public
3 records by accessing any computer, computer system, or network
4 that is operated by this state, a political subdivision of
5 this state, or a medical institution.

6 (8) Giving a password, identifying code, personal
7 identification number, debit card number, bank account number,
8 or other confidential information about a computer security
9 system to another person without the consent of the person
10 using the computer security system to restrict access to a
11 computer, computer network, computer system, or data.

12 (b) (1) Except as otherwise provided in this
13 subsection, the offense of computer tampering is a Class A
14 misdemeanor, punishable as provided by law.

15 (2) If the actor's intent is to obtain a benefit, or
16 defraud or harm another, the offense is a Class C felony,
17 punishable as provided by law.

18 (3) If any violation results in a victim expenditure
19 of greater than two thousand five hundred dollars (\$2,500), or
20 if there is an interruption or impairment of governmental
21 operations or public communication, transportation, or supply
22 of water, gas, or other public or utility service, then the
23 offense is a Class B felony, punishable as provided by law.

24 (4) If any violation results in a victim expenditure
25 of greater than one hundred thousand dollars (\$100,000), or if
26 the committed offense causes physical injury to any person who

1 is not involved in the act, then the offense is a Class A
2 felony, punishable as provided by law.

3 (c) A prosecution for a violation of this section
4 may be tried in any of the following:

5 (1) The county in which the victimized computer,
6 computer system, or network is located.

7 (2) The county in which the computer, computer
8 system, or network that was used in the commission of the
9 offense is located or in which any books, records, documents,
10 property, financial instruments, computer software, data,
11 access devices, or instruments of the offense were used.

12 (3) The county in which any authorized user was
13 denied service or in which an authorized user's service was
14 interrupted.

15 (4) The county in which critical infrastructure
16 resources were tampered with or affected.

17 Section 4. (a) A person commits the crime of encoded
18 data fraud by:

19 (1) Knowingly and with the intent to defraud,
20 possessing a scanning device; or knowingly and with intent to
21 defraud, using or attempting to use a scanning device to
22 access, read, obtain, memorize, or store, temporarily or
23 permanently, information encoded on an identification document
24 by means of magnetic strip, integrated circuit, or radio
25 frequency identification tag without the permission of the
26 authorized user or issuer of the identification document.

1 (2) Knowingly and with the intent to defraud,
2 possessing a reencoder; or knowingly and with intent to
3 defraud, using or attempting to use a reencoder to place
4 encoded information on an identification document by means of
5 magnetic strip, integrated circuit, or radio frequency
6 identification tag without the permission of the authorized
7 user or issuer of the identification document from which the
8 information is being reencoded.

9 (b) Any person violating this section, upon
10 conviction, shall be guilty of a Class C felony.

11 (c) Any scanning device or reencoder owned by the
12 defendant and possessed or used in violation of this section
13 may be seized and be destroyed as contraband by the
14 investigating law enforcement agency by which the scanning
15 device or reencoder was seized.

16 Section 5. (a) A person commits the crime of
17 phishing if the person by means of an Internet web page,
18 electronic mail message, or otherwise using the Internet,
19 solicits, requests, or takes any action to induce another
20 person to provide identifying information by representing that
21 the person, either directly or by implication, is a business,
22 without the authority or approval of the business.

23 (b) Any person violating this section, upon
24 conviction, shall be guilty of a Class C felony. Multiple
25 violations resulting from a single action or act shall
26 constitute one violation for the purposes of this section.

1 (c) The following persons may bring an action
2 against a person who violates or is in violation of this
3 section:

4 (1) A person who is engaged in the business of
5 providing Internet access service to the public, owns a web
6 page, or owns a trademark, and is adversely affected by a
7 violation of this section.

8 (2) An individual who is adversely affected by a
9 violation of this section.

10 (d) In any criminal proceeding brought pursuant to
11 this section, the crime shall be considered to be committed in
12 any county in which any part of the crime took place,
13 regardless of whether the defendant was ever actually present
14 in that county, or in the county of residence of the person
15 who is the subject of the identification documents or
16 identifying information.

17 (e) The Attorney General, the district attorney, a
18 designee of the district attorney, or any person aggrieved by
19 a violation of subsection (a) may file a civil action in
20 circuit court to enforce this section and to enjoin further
21 violations of this section. The Attorney General, district
22 attorney, a designee of the district attorney, or such
23 aggrieved person may recover actual damages or twenty-five
24 thousand dollars (\$25,000), whichever is greater, for each
25 violation of subsection (a).

26 (f) In a civil action under subsection (e), the
27 court may increase the damage award to an amount equal to not

1 more than three times the award provided in subsection (d) if
2 the court determines that the defendant has engaged in a
3 pattern and practice of violating subsection (a).

4 (g) Proceeds from an action under subsection (e)
5 shall first be used for payment of all proper expenses,
6 including court costs, of the proceedings for the civil action
7 with the remaining proceeds payable first towards the
8 restitution of any victims, as determined by the court. Any
9 remaining proceeds shall be awarded equally between the State
10 General Fund and the office of the Attorney General, the
11 office of the district attorney bringing the action, or both.

12 (h) An interactive computer service provider shall
13 not be held liable or found in violation of this section for
14 identifying, removing, or disabling access to an Internet web
15 page or other online location that such provider believes in
16 good faith is being used to engage in a violation of this
17 section.

18 Section 6. (a) A person commits the crime of
19 electronic harassment if, with intent to harass, annoy, or
20 alarm any person, he or she transmits, posts, displays, or
21 disseminates, by or through an electronic communication
22 device, radio, computer, Internet, or other similar means, to
23 any person, a communication, image, or information, which is
24 based on the actual or perceived traits or characteristics of
25 that person, which creates any of the following conditions:

26 (1) Places that person in reasonable fear or harm to
27 his or her person or property.

1 (2) Has a substantial and detrimental effect on that
2 person's physical or mental health.

3 (3) Has the effect of substantially interfering with
4 that person's academic performance, employment, or other
5 community activities or responsibilities.

6 (4) Has the effect of substantially interfering with
7 that person's ability to participate in or benefit from any
8 academic, professional, or community-based services,
9 activities, or privileges.

10 (5) Has the effect of causing substantial
11 embarrassment or humiliation within an academic or
12 professional community.

13 (b) Any person violating this section, upon
14 conviction, shall be guilty of a Class A misdemeanor.

15 Section 7. (a) A person commits the crime of
16 cyberstalking if he or she does any of the following:

17 (1) Uses in electronic mail or electronic
18 communication any words or language threatening to inflict
19 physical injury to any person or to that person's child,
20 sibling, spouse, dependent, or another individual living in
21 the same household as the victim; or for the purpose of
22 extorting money or other things of value from any person; or
23 damage to the property of any person.

24 (2) Electronically mails or electronically
25 communicates to another repeatedly, whether or not
26 conversation ensues, for the purpose of threatening,
27 terrifying, or harassing any person.

1 (3) Electronically mails or electronically
2 communicates to another and knowingly makes any false
3 statement concerning death, injury, illness, disfigurement,
4 indecent conduct, or criminal conduct of the person
5 electronically mailed or of any member of the person's family
6 or household with the intent to threaten, terrify, or harass.

7 (4) Knowingly permits an electronic communication
8 device under the person's control to be used for any purpose
9 prohibited by this section.

10 (b) Except as otherwise provided in subsections (c)
11 and (d), any person violating this section, upon conviction,
12 shall be guilty of a Class A misdemeanor.

13 (c) If any of the following apply, the person is
14 guilty of a Class C felony:

15 (1) The offense is in violation of a restraining
16 order and the person has received actual notice of that
17 restraining order or posting the message is in violation of an
18 injunction or preliminary injunction.

19 (2) The offense is in violation of a condition of
20 probation, a condition of parole, a condition of pretrial
21 release, or a condition of release on bond pending appeal.

22 (3) The actor has been convicted and a credible
23 threat is communicated to that actor's victim or witness, a
24 family member of that victim or witness, or another individual
25 living in the same household as that victim or witness.

26 (4) The person has been previously convicted of
27 violating this section or a substantially similar law of

1 another state, a political subdivision of another state, or of
2 the United States.

3 (d) This section does not apply to any peaceable,
4 nonviolent, or nonthreatening activity intended to express
5 political views or to provide lawful information to others.
6 This section shall not be construed to impair any
7 constitutionally protected activity, including speech,
8 protest, or assembly.

9 Section 8. (a) A law enforcement officer, a
10 prosecuting attorney, or the Attorney General may require the
11 disclosure of stored wire or electronic communications, as
12 well as transactional records pertaining thereto, to the
13 extent and under the procedures and conditions provided for by
14 the laws of the United States.

15 (b) A provider of electronic communication service
16 or remote computing service shall provide the contents of, and
17 transactional records pertaining to, wire and electronic
18 communications in its possession or reasonably accessible
19 thereto when a requesting law enforcement officer, a
20 prosecuting attorney, or the Attorney General complies with
21 the provisions for access thereto set forth by the laws of the
22 United States.

23 (c) Search warrants for production of stored wire or
24 electronic communications and transactional records pertaining
25 thereto shall have statewide application or application as
26 provided by the laws of the United States when issued by a

1 judge with jurisdiction over the criminal offense under
2 investigation and to which such records relate.

3 (d) This section specifically authorizes any law
4 enforcement official, prosecuting attorney, or the Attorney
5 General to issue a subpoena to obtain any stored electronic
6 records governed by 18 U.S.C. § 2703(b) et seq, and any
7 successor statute. The subpoena shall be issued with a showing
8 that the subpoenaed material relates to a pending
9 investigation.

10 (e) Violation of this section shall be punishable as
11 contempt.

12 Section 9. (a) An Alabama corporation that provides
13 electronic communication services or remote computing services
14 to the general public, when served with a warrant issued by
15 another state to produce records that would reveal the
16 identity of the customers using those services, data stored
17 by, or on behalf of, the customer, the customer's usage of
18 those services, the recipient or destination of communications
19 sent to or from those customers, or the content of those
20 communications, shall produce those records as if that warrant
21 had been issued by an Alabama court.

22 (b) Violation of this section shall be punishable as
23 contempt.

24 Section 10. (a) On conviction of a violation of this
25 section, the court shall order that any computer, computer
26 system, computer network, instrument of communication,
27 software or data that was owned or used by the defendant and

1 that was used in the commission of the offense be forfeited to
2 the State of Alabama and sold, destroyed, or otherwise
3 properly disposed. If the defendant is a minor, it also
4 includes the above listed property of the parent or guardian
5 of the defendant. The manner, method, and procedure for the
6 forfeiture and condemnation or forfeiture of such thing shall
7 be the same as that provided by law for the confiscation or
8 condemnation or forfeiture of automobiles, conveyances, or
9 vehicles in which alcoholic beverages are illegally
10 transported.

11 (b) When property is forfeited under this section,
12 the court may award the property to any state, county, or
13 municipal law enforcement agency or department who
14 participated in the investigation or prosecution of the
15 offense given rise to the seizure. The recipient law
16 enforcement agency shall use such property for law enforcement
17 purposes but, at its discretion, may transfer the tangible
18 property to another governmental department or agency to
19 support crime prevention. The agencies may sell that which is
20 not required to be destroyed and which is not harmful to the
21 public. The proceeds from a sale authorized by this act shall
22 be used first for payment of all proper expenses of the
23 proceedings for forfeiture and sale and the remaining proceeds
24 from the sale shall be awarded and distributed by the court to
25 the participating agencies to be used exclusively for law
26 enforcement purposes.

1 Section 11. A person who is subject to prosecution
2 under this section and any other law of this state may be
3 prosecuted under either or both laws.

4 Section 12. Article 5, consisting of Sections
5 13A-8-100, 13A-8-101, 13A-8-102, and 13A-8-103 of Chapter 8 of
6 Title 13A of, the Code of Alabama 1975, relating to computer
7 crimes, is repealed.

8 Section 13. Although this bill would have as its
9 purpose or effect the requirement of a new or increased
10 expenditure of local funds, the bill is excluded from further
11 requirements and application under Amendment 621, now
12 appearing as Section 111.05 of the Official Recompilation of
13 the Constitution of Alabama of 1901, as amended, because the
14 bill defines a new crime or amends the definition of an
15 existing crime.

16 Section 14. This act shall become effective on the
17 first day of the third month following its passage and
18 approval by the Governor, or its otherwise becoming law.