ACT NO. 2012-432

HB400

142837-2

By Representative DeMarco

RFD: Judiciary

First Read: 23-FEB-12

1

2 ENROLLED, An Act,

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

15 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

16 Section 1. This act may be cited as The Alabama
17 Digital Crime Act.

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

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

24 (2) COMPUTER. An electronic, magnetic, optical,
25 electrochemical, or other high speed data processing device or

system that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

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

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

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

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

(7) COMPUTER SOFTWARE. A set of instructions or 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) EXCEEDS AUTHORIZATION OF USE. Accessing a
17 computer, computer network, or other digital device with
18 actual or perceived authorization, and using such access to
19 obtain or alter information that the accessor is not entitled
20 to obtain or alter.
21 (12) FINANCIAL INSTRUMENT. Includes, but is not
22 limited to, any check, cashier's check, draft, warrant, money
23 order, certificate of deposit, negotiable instrument, letter
24 of credit, bill of exchange, credit or debit card, transaction

1 authorization mechanism, marketable security, or any computer
2 system representation thereof.
3 (13) HARM. Partial or total alteration, damage, or
4 erasure of stored data, interruption of computer services,
5 introduction of a virus, or any other loss, disadvantage, or
6 injury that might reasonably be suffered as a result of the
7 actor's conduct.
8 (14) IDENTIFICATION DOCUMENT. Any document
9 containing data that is issued to an individual and which that
10 individual, and only that individual, uses alone or in
11 conjunction with any other information for the primary purpose
12 of establishing his or her identity or accessing his or her
13 financial information or benefits. Identification documents
14 specifically include, but are not limited to, the following:
15 a. Government issued driver's licenses or
16 identification cards.
17 b. Payment cards such as credit cards, debit cards,
18 and ATM cards.
19 c. Passports.
20 d. Health insurance or benefit cards.
21 e. Identification cards issued by educational
22 institutions.
23 f. Identification cards for employees or
24 contractors.

1 g. Benefit cards issued in conjunction with any
2 government supported aid program.
3 h. Library cards issued by any public library.
4 (15) IDENTIFYING INFORMATION. Specific details that
5 can be used to access a person's financial accounts, obtain
6 identification, or to obtain goods or services, including, but
7 not limited to:
8 a. Social Security number.
9 b. Driver's license number.
10 c. Bank account number.
11 d. Credit card or debit card number.
12 e. Personal identification number (PIN).
13 f. Automated or electronic signature.
14 g. Unique biometric data.
15 h. Account password.
16 (16) INTEGRATED CIRCUIT CARD. Also known as a smart
17 card or chip card, a pocket sized, plastic card with embedded
18 integrated circuits used for data storage or special purpose
19 processing used to validate personal identification numbers
20 (PINs), authorize purchases, verify account balances and store
21 personal records. When inserted into a reader, it transfers
22 data to and from a central computer.
23 (17) OWNER. An owner or lessee of a computer or a
24 computer network, or an owner, lessee, or licensee of computer
25 data, computer programs, or computer software.

1 (18) PROPERTY. Includes a financial instrument,
2 data, databases, data while in transit, computer software,
3 computer programs, documents associated with computer systems
4 and computer programs, or copies whether tangible or
5 intangible.
6 (19) RADIO FREQUENCY IDENTIFICATION (RFID). A
7 technology that uses radio waves to transmit data remotely
8 from an RFID tag, through a reader, from identification
9 documents. It is used in contactless integrated circuit cards,
10 also known as proximity cards.
11 (20) RADIO FREQUENCY IDENTIFICATION (RFID) TAGS.
12 Also known as RFID labels, the hardware for an RFID system
13 that electronically stores and processes information, and
14 receives and transmits the signal.
15 (21) REENCODER. An electronic device that places
16 encoded information from the magnetic strip, integrated
17 circuit, RFID tag of an identification document onto the
18 magnetic strip, integrated circuit, or RFID tag of a different
19 identification document.
20 (22) SCANNING DEVICE. A scanner, reader, or any
21 other electronic device that is used to access, read, scan,
22 obtain, memorize, or store, temporarily or permanently,
23 information encoded on the magnetic strip, integrated circuit,
24 or RFID tag of an identification document.

1 (23) VIRUS. Means an unwanted computer program or
2 other set of instructions inserted into a computer's memory,
3 operating system, or program that is specifically constructed
4 with the ability to replicate itself or to affect the other
5 programs or files in the computer by attaching a copy of the
6 unwanted program or other set of instructions to one or more
7 computer programs or files.
8 (24) WEB PAGE. A location that has a single uniform
9 resource locator or other single location with respect to the
10 Internet.
11 Section 3. (a) A person who acts without authority
12 or who exceeds authorization of use commits the crime of
13 computer tampering by knowingly:
14 (1) Accessing and altering, damaging, or destroying
15 any computer, computer system, or computer network.
16 (2) Altering, damaging, deleting, or destroying
17 computer programs or data.
18 (3) Disclosing, using, controlling, or taking
19 computer programs, data, or supporting documentation residing
20 in, or existing internal or external to, a computer, computer
21 system, or network.
22 (4) Directly or indirectly introducing a computer
23 contaminator or a virus into any computer, computer system, or
24 network.

1 (5) Disrupting or causing the disruption of a
2 computer, computer system, or network services or denying or
3 causing the denial of computer or network services to any
4 authorized user of a computer, computer system, or network.
5 (6) Preventing a computer user from exiting a site,
6 computer system, or network-connected location in order to
7 compel the user's computer to continue communicating with,
8 connecting to, or displaying the content of the service, site,
9 or system.
10 (7) Obtaining any information that is required by
11 law to be kept confidential or any records that are not public
12 records by accessing any computer, computer system, or network
13 that is operated by this state, a political subdivision of
14 this state, or a medical institution.
15 (8) Giving a password, identifying code, personal
16 identification number, debit card number, bank account number,
17 or other confidential information about a computer security
18 system to another person without the consent of the person
19 using the computer security system to restrict access to a
20 computer, computer network, computer system, or data.
21 (b)(1) Except as otherwise provided in this
22 subsection, the offense of computer tampering is a Class A
23 misdemeanor, punishable as provided by law. Subsection (a)
24 does not apply to any acts which are committed by a person
25 within the scope of his or her lawful employment. For purposes

of this section, a person acts within the scope of his of her employment when he or she performs acts which are reasonably necessary to the performance of his or her work assignment.

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

(3) If any violation results in a victim expenditure of greater than two thousand five hundred dollars ($2,500), or if the actor's intent is to obtain a benefit, commit an unlawful act, or defraud or harm another and there is an interruption or impairment of governmental operations or public communication, transportation, or supply of water, gas, or other public or utility service, then the offense is a Class B felony, punishable as provided by law.

(4) If any violation results in a victim expenditure of greater than one hundred thousand dollars ($100,000), or if the committed offense causes physical injury to any person who is not involved in the act, then the offense is a Class A felony, punishable as provided by law.

(5) If any violation relates to access to an Alabama Criminal Justice Information Center information system or to data regulated under the authority of the Alabama Criminal Justice Information Center Commission, the offense is a Class B felony, punishable as provided by law. Misuse of each

individual record constitutes a separate offense under this subsection.

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

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

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

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

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

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

(1) Knowingly and with the intent to commit an unlawful act or to defraud, possessing a scanning device; or knowingly and with intent to commit an unlawful act or defraud, using or attempting to use a scanning device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on an identification document by means of magnetic strip, integrated circuit, or radio

1 frequency identification tag without the permission of the
2 authorized user or issuer of the identification document.
3 (2) Knowingly and with the intent to commit an
4 unlawful act or to defraud, possessing a reencoder; or
5 knowingly and with intent to commit an unlawful act or
6 defraud, using or attempting to use a reencoder to place
7 encoded information on an identification document by means of
8 magnetic strip, integrated circuit, or radio frequency
9 identification tag without the permission of the authorized
10 user or issuer of the identification document from which the
11 information is being reencoded.
12 (b) Any person violating this section, upon
13 conviction, shall be guilty of a Class C felony.
14 (c) Any scanning device or reencoder owned by the
15 defendant and possessed or used in violation of this section
16 may be seized and be destroyed as contraband by the
17 investigating law enforcement agency by which the scanning
18 device or reencoder was seized.
19 Section 5. (a) A person commits the crime of
20 phishing if the person by means of an Internet web page,
21 electronic mail message, or otherwise using the Internet,
22 solicits, requests, or takes any action to induce another
23 person to provide identifying information by representing that
24 the person, either directly or by implication, is a business,
25 without the authority or approval of the business.

1 (b) Any person violating this section, upon
2 conviction, shall be guilty of a Class C felony. Multiple
3 violations resulting from a single action or act shall
4 constitute one violation for the purposes of this section.
5 (c) The following persons may bring an action
6 against a person who violates or is in violation of this
7 section:
8 (1) A person who is engaged in the business of
9 providing Internet access service to the public, owns a web
10 page, or owns a trademark, and is adversely affected by a
11 violation of this section.
12 (2) An individual who is adversely affected by a
13 violation of this section.
14 (d) In any criminal proceeding brought pursuant to
15 this section, the crime shall be considered to be committed in
16 any county in which any part of the crime took place,
17 regardless of whether the defendant was ever actually present
18 in that county, or in the county of residence of the person
19 who is the subject of the identification documents or
20 identifying information.
21 (e) The Attorney General or the district attorney
22 may file a civil action in circuit court to enforce this
23 section and to enjoin further violations of this section. The
24 Attorney General or the district attorney may recover actual

1 damages or twenty-five thousand dollars ($25,000), whichever
2 is greater, for each violation of subsection (a).
3 (f) In a civil action under subsection (e), the
4 court may increase the damage award to an amount equal to not
5 more than three times the award provided in subsection (d) if
6 the court determines that the defendant has engaged in a
7 pattern and practice of violating subsection (a).
8 (g) Proceeds from an action under subsection (e)
9 shall first be used for payment of all proper expenses,
10 including court costs, of the proceedings for the civil action
11 with the remaining proceeds payable first towards the
12 restitution of any victims, as determined by the court. Any
13 remaining proceeds shall be awarded equally between the State
14 General Fund and the office of the Attorney General, the
15 office of the district attorney bringing the action, or both.
16 (h) An interactive computer service provider shall
17 not be held liable or found in violation of this section for
18 identifying, removing, or disabling access to an Internet web
19 page or other online location that such provider reasonably
20 believes by clear and convincing evidence that it is being
21 used to engage in a violation of this section.
22 Section 6. (a) A law enforcement officer, a
23 prosecuting attorney, or the Attorney General may require the
24 disclosure of stored wire or electronic communications, as
25 well as transactional records and subscriber information

1 pertaining thereto, to the extent and under the procedures and
2 conditions provided for by the laws of the United States.
3 (b) A provider of electronic communication service
4 or remote computing service shall provide subscriber
5 information as well as the contents of, and transactional
6 records pertaining to, wire and electronic communications in
7 its possession or reasonably accessible thereto when a
8 requesting law enforcement officer, a prosecuting attorney, or
9 the Attorney General complies with the provisions for access
10 thereto set forth by the laws of the United States.
11 (c) Warrants or appropriate orders for production of
12 stored wire or electronic communications and transactional
13 records pertaining thereto shall have statewide application or
14 application as provided by the laws of the United States when
15 issued by a judge with jurisdiction over the criminal offense
16 under investigation or to which such records relate.
17 (d) This section specifically authorizes any law
18 enforcement official, prosecuting attorney, or the Attorney
19 General to issue a subpoena to obtain any stored electronic
20 records governed by 18 U.S.C. § 2703(b) et seq, and any
21 successor statute. The subpoena shall be issued with a showing
22 that the subpoenaed material relates to an investigation.
23 (e) Intentional violation of this section shall be
24 punishable as contempt.

1 Section 7. (a) An Alabama corporation or business
2 entity that provides electronic communication services or
3 remote computing services to the general public, when served
4 with a warrant issued by another state to produce records that
5 could reveal the identity of the customers using those
6 services, data stored by, or on behalf of, the customer, the
7 customer's usage of those services, the recipient or
8 destination of communications sent to or from those customers,
9 or the content of those communications, shall produce those
10 records as if that warrant had been issued by an Alabama
11 court.
12 (b) Intentional violation of this section shall be
13 punishable as contempt.
14 Section 8. (a) On conviction of a violation of this
15 act or any other violation of the criminal laws of Alabama,
16 the court shall order that any computer, computer system,
17 computer network, instrument of communication, software or
18 data that was owned or used by the defendant with the owner's
19 knowledge of the unlawful act or where the owner had reason to
20 know of the unlawful act, and that was used in the commission
21 of the offense be forfeited to the State of Alabama and sold,
22 destroyed, or otherwise properly disposed. If the defendant is
23 a minor, it also includes the above listed property of the
24 parent or guardian of the defendant. The manner, method, and
25 procedure for the forfeiture and condemnation or forfeiture of

1 such thing shall be the same as that provided by law for the
2 confiscation or condemnation or forfeiture of automobiles,
3 conveyances, or vehicles in which alcoholic beverages are
4 illegally transported. If the computer, computer system,
5 computer network, instrument of communication, software, or
6 data that was used by a defendant, in conjunction with a
7 violation of this act, is owned or leased by the defendant's
8 employer or a client or vendor of the defendant's employer and
9 such owner or lessor did not authorize the activity violating
10 the act, then this section shall not apply.
11 (b) When property is forfeited under this act or any
12 other violation of the criminal laws of Alabama, the court may
13 award the property to any state, county, or municipal law
14 enforcement agency or department who participated in the
15 investigation or prosecution of the offense given rise to the
16 seizure. The recipient law enforcement agency shall use such
17 property for law enforcement purposes but, at its discretion,
18 may transfer the tangible property to another governmental
19 department or agency to support crime prevention. The agencies
20 may sell that which is not required to be destroyed and which
21 is not harmful to the public. The proceeds from a sale
22 authorized by this act shall be used first for payment of all
23 proper expenses of the proceedings for forfeiture and sale and
24 the remaining proceeds from the sale shall be awarded and

1 distributed by the court to the participating agencies to be
2 used exclusively for law enforcement purposes.
3 (c) Pursuant to Section 15-18-67 of the Code of
4 Alabama 1975, and in addition to any other cost ordered
5 pursuant to law, the district attorney may request and the
6 court may order the defendant to pay the cost of prosecution
7 or investigation, or both. Restitution shall include any and
8 all costs associated with the violation of the criminal laws
9 of this state.
10 Section 9. A person who is subject to prosecution
11 under this section and any other law of this state may be
12 prosecuted under either or both laws.
13 Section 10. Nothing in this act prohibits any
14 lawfully authorized investigative, protective, or intelligence
15 activity of a law enforcement agency of this state or a
16 political subdivision of this state or a law enforcement
17 agency of the United States or of an intelligence agency of
18 the United States.
19 Section 11. Article 5, consisting of Sections
20 13A-8-100, 13A-8-101, 13A-8-102, and 13A-8-103 of Chapter 8 of
21 Title 13A of, the Code of Alabama 1975, relating to computer
22 crimes, is repealed.
23 Section 12. Although this bill would have as its
24 purpose or effect the requirement of a new or increased
25 expenditure of local funds, the bill is excluded from further

requirements and application under Amendment 621, now appearing as Section 111.05 of the Official Recompilation of the Constitution of Alabama of 1901, as amended, because the bill defines a new crime or amends the definition of an existing crime.

Section 13. This act shall become effective on the first day of the third month following its passage and approval by the Governor, or its otherwise becoming law.

1

2

3

4 Speaker of the House of Representatives

5 Kay Ivey

6 President and Presiding Officer of the Senate

7 House of Representatives

8 I hereby certify that the within Act originated in
9 and was passed by the House 15-MAR-12, as amended.
10
11 Greg Pappas
12 Clerk
13

14

15	Senate	03-MAY-12	Amended and Passed
16	House	08-MAY-12	Passed, as amended by Conference Committee Report
17	Senate	09-MAY-12	Passed, as amended by Conference Committee Report

APPROVED May 15, 2012
TIME 6:18 p.m.
Robert Bentley
GOVERNOR

Alabama Secretary Of State

Act Num....: 2012-432
Bill Num...: H-400

Recv'd 05/16/12 01:19pmSLF

ONSOR
DeMarco
-SPONSORS

HOUSE ACTION

I HEREBY CERTIFY THAT THE RESOLUTION AS REQUIRED IN SECTION C OF ACT NO. 81-889 WAS ADOPTED AND IS ATTACHED TO THE BILL, H.B. 400

YEAS 95 NAYS 0

GREG PAPPAS, Clerk

I HEREBY CERTIFY THAT THE NOTICE & PROOF IS ATTACHED TO THE BILL, H.B. _____ AS REQUIRED IN THE GENERAL ACTS OF ALABAMA, 1975 ACT NO. 919.

GREG PAPPAS, Clerk

CONFERENCE COMMITTEE

House Conferees DEMARCO
ENGLAND
POOLE

SENATE ACTION

DATE: 3-20- 2012

RD 1 RFD Judy

This Bill was referred to the Standing Committee of the Senate on Judy and was acted upon by such Committee in session and is by order of the Committee returned therefrom with a favorable report w/amend(s) 1 w/sub ____ by a vote of yeas 11 nays 0 abstain 0 this 11 day of April 2012

_____, Chairperson

DATE: 4-12 2012

RF FAV/AMD RD 2 CAL

DATE: 2012

RE-REFERRED ☐ RE-COMMITTED ☐

Committee _____

I hereby certify that the Resolution as required in Section C of Act No. 81-889 was adopted and is attached to the Bill, HB 400

YEAS ____ NAYS ____

PATRICK HARRIS, Secretary

FURTHER SENATE

SENATE ACTION
(Continued)

DATE: S RD 3 at
PASSED PASSED AS AMENDED

YEAS 4 NAYS 0

And was ordered returned forthwith to the H

PATRICK HA

Sec

DATE:

INDEFINITELY POSTPONED YEAS NAY

DATE:

RECONSIDERED YEAS NAY

CONFERENCE COMMITTEE

Senate Conferees _____

This bill having been referred to the Committe
Rules pursuant to Senate Rule 23 is reported t
Senate for assignment to the Committee on:

This _____ day of _____, 20__

_____, Chairper

Date: _____

Rereferred

Committee: _____