Ala. Code 1975, § 13A-8-112(b)(4)
Computer Tampering
(Victim Expenditure)

The defendant is charged with computer tampering.

A person commits the crime of computer tampering if he/she acts without authority or exceeds authorization of use and knowingly does any of the following: **[Read as appropriate]:**

(1) Accesses and alters, damages, or destroys a computer, computer system, or computer network;

(2) Alters, damages, deletes or destroys computer programs or data;

(3) Discloses, uses, controls, or takes computer programs, data, or supporting documentation residing in, or existing internal or external to, a computer, computer system, or network;

(4) Directly or indirectly introduces a computer contaminator or a virus into any computer, computer system, or network;

(5) Disrupts or causes the disruption of a computer, computer system, or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system, or network;

(6) Prevents a computer user from exiting a site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system;

(7) Obtains information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system, or network that is operated by this state, a political subdivision of this state, or a medical institution;

(OR)

(8) Gives a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the consent of the person using the computer security system to restrict access to a computer, computer network, computer system, or data;

resulting in a victim expenditure of greater than $100,00.

To convict, the State must prove beyond a reasonable doubt each of the following elements:

(1) The defendant acted without authority or exceeded authority of use;

(2) The defendant **[Read as appropriate]:**

(a) Accessed and altered, damaged, or destroyed a computer,

computer system, or computer network;

(b) Altered, damaged, deleted, or destroyed computer programs or data;

(c) Disclosed, used, controlled, or took computer programs, data, or supporting documentation residing in, or existing internal or external to, a computer, computer system, or network;

(d) Directly or indirectly introduced a computer contaminator or a virus into any computer, computer system, or network;

(e) Disrupted or caused the disruption of a computer, computer system, or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system, or network;

(f) Prevented a computer user from exiting a site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system;

(g) Obtained information that was required by law to be kept confidential or records that were not public records by accessing any computer, computer system, or network that is operated by this state, a political subdivision of this state, or a medical institution;

(OR)

(h) Gave a password, identifying code, personal identification number, debit card number, bank account number, or other confidential information about a computer security system to another person without the consent of the person using the computer security system to restrict access to a computer, computer network, computer system, or data;

(3) The Defendant did so knowingly; **(AND)**

(4) The Defendant's act resulted in a victim expenditure of greater than $100,000.

[Read as appropriate]:

To *access* means to gain entry to, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer system, or computer network. [13A-8-111(1)]

A *computer* is an electronic, magnetic, optical, 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. [13A-8-111(2)]

A *computer network* is the interconnection of two or more computers or computer systems that transmit data over communication circuits connecting them. [13A-8-111(3)]

A *computer program* is 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. [13A-8-111(4)]

A *computer security system* is 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. [13A-8-111(5)]

Computer services are 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. [13A-8-111(6)]

Computer software is a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer, computer system, or computer network to perform specific functions. [13A-8-111(7)]

Computer system is a set of related or interconnected computer or computer network equipment, devices and software. [13A-8-111(8)]

Data is a representation of information, knowledge, facts, concepts, or instructions, which are prepared and are intended for use in a computer, computer system, or computer network. Data may be in any form, in storage media, or as stored in the memory of the computer or in transit. [13A-8-111(9)]

Electronic mail message is a message sent to a unique destination that consists of a unique user name or mailbox and a reference to an Internet domain, whether or not displayed, to which such message can be sent or delivered. [13A-8-111(10)]

Exceeds authorization of use is accessing a computer, computer network, or other digital device with actual or perceived authorization, and using such access to obtain or alter information that the accessor is not entitled to obtain or alter. [13A-8-111(11)]

A *financial instrument* includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof. [13A-8-111(12)]

Harm is a partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a virus, or any other loss,

disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct. [13A-8-111(13)]

An *identification document* is any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity or accessing his or her financial information or benefits.
Identification documents specifically include, but are not limited to, the following:

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

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

c. Passports.

d. Health insurance or benefit cards.

e. Identification cards issued by educational institutions.

f. Identification cards for employees or contractors.

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

h. Library cards issued by any public library.

[13A-8-111(14)]

Identifying information are specific details that can be used to access a person's financial accounts, obtain identification, or to obtain goods or services, including, but not limited to:

a. Social Security number.

b. Driver's license number.

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.

[13A-8-111(15)]

An *integrated circuit card* is 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. [13A-8-111(16)]

An *owner* is 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. [13A-8-111(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. [13A-8-111(18)]

Radio Frequency Identification (RFID) is 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. [13A-8-111(19)]

Radio Frequency Identification (RFID) Tags are also known as RFID labels and are the hardware for an RFID system that electronically stores and processes information, and receives and transmits the signal. [13A-8-111(20)]

A *reencoder* is an electronic device that places encoded information from the magnetic strip, integrated circuit, RFID tag of an identification document onto the magnetic strip, integrated circuit, or RFID tag of a different identification document. [13A-8-111(21)]

A *scanning device* is a scanner, reader, or any other electronic device that is used to access, read, scan, obtain, memorize, or store, temporarily or permanently, information encoded on the magnetic strip, integrated circuit, or RFID tag of an identification document. [13A-8-111(22)]

A *virus* means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.
[13A-8-111(23)]

A *web page* is a location that has a single uniform resource locator or other single location with respect to the Internet. [13A-8-111(24)]

[Read as appropriate]: This law does not apply to any acts which are committed by a person within the scope of his/her lawful employment. A person acts within the scope of his/her employment when he/she performs acts which are reasonably necessary to the performance of his/her work assignment.
[13A-8-112(b)(1)]

A person acts *knowingly* with respect to conduct or to a circumstance described by a statute defining an offense he/she is aware that his/her conduct is of that nature or that the circumstance exists. [13A-2-2(2)]

If you find from the evidence that the State has proved beyond a reasonable doubt each of the elements of the offense of computer tampering, then you shall find

the defendant guilty of computer tampering.

If you find from the evidence that the State has failed to prove beyond a reasonable doubt any one or more of the elements of computer tampering, then you shall find the defendant not guilty of computer tampering.

[Approved October 18, 2019].