OLR Bill Analysis
sSB 811

AN ACT INCREASING PENALTIES FOR COMPUTER CRIMES AGAINST FINANCIAL INSTITUTIONS AND THEIR CUSTOMERS.

SUMMARY
This bill increases the penalty for committing certain computer crimes against financial institutions, including unauthorized removal or destruction of electronic financial information, to a Class A felony, punishable by 10 to 25 years imprisonment, up to $20,000 fine, or both. The bill’s increased penalty applies to computer crimes committed against a financial institution or any computers, networks, programs, or software it owns, leases, or licenses.

Under current law, persons committing one of these computer crimes is guilty of a (1) Class B misdemeanor, (2) Class A misdemeanor if their reckless disregard for their actions causes over $2,500 in damage and, (3) Class D felony if their malicious actions cause over $2,500 in damage. The maximum prison term for these crimes under current law thus ranges from six months to five years, and the maximum fine ranges from $1,000 to $5,000.

(By law, unauthorized access and damage to computer systems is already punishable under a different statute, and in some cases may constitute a Class B felony, see BACKGROUND).

The bill also modifies certain definitions related to computer crimes to specify their applicability to financial institution data and financial instruments.

EFFECTIVE DATE: October 1, 2019

FINANCIAL INSTITUTION
Under the bill, a “financial institution” conducts business in
Connecticut as a:

1. Federal Deposit Insurance Corporation insured bank or National Credit Union Administration insured credit union,
2. broker dealer registered with the federal Securities and Exchange Commission (SEC) pursuant to federal law,
3. Connecticut licensed insurer, or
4. investment advisory firm registered with either the SEC or Connecticut Department of Banking.

**COMPUTER CRIMES**

Existing law prohibits a person using a computer or computer network without authority and with the intent to:

1. remove, halt, or disable computer data, programs, or software from a network;
2. cause a computer to malfunction;
3. alter or erase data, programs, or software;
4. create or alter financial instruments or electronic funds transfers;
5. physically injure property;
6. copy or cause to be copied any printed or electronic computer data, programs, or software residing in, communicated by, or produced by a computer or computer network; or
7. falsify or forge electronic mail transmission or routing information to send unsolicited bulk electronic mail or knowingly sell, give, distribute, or possess with the intent to sell, give, or distribute software associated with falsifying electronic mail transmission and routing information (CGS § 53-451).
The bill’s increased penalty applies to any of these crimes committed against a financial institution or any computers, networks, programs, or software it owns or leases.

The bill also explicitly provides that, for purposes of these computer crimes:

1. “Computer data” includes nonpublic personal information of people who use or apply for financial institution products or services; and

2. “Financial instruments” include devices, instruments, or instructions used to access (a) loan or deposit account information or (b) money, securities, or similar property held by a financial institution for the benefit of another person in a custodial, trust, or fiduciary capacity.

BACKGROUND

Related Crimes

By law, unauthorized access to a computer system, theft or interruption of computer services, and misuse of computer system information ranges from a Class B misdemeanor (for damages of $500 or less) to a Class B felony (for damages exceeding $10,000) (CGS § 53a-250 et seq.). Committing a computer crime in furtherance of a terrorist purpose is a Class B felony with a mandatory minimum of five years in some circumstances (CGS § 53a-301).

COMMITTEE ACTION

Banking Committee

Joint Favorable Substitute
Yea 15  Nay 0  (03/05/2019)