

SB

259

Overview and Explanation of Changes SB 259 (Jud)

Expansion of the previous bill. It uses some federal language.

We have looked into the concerns that Senator Halford expressed about victim's rights (credit reporting) in this bill. Unfortunately this language is criminal and according to legal, victim rights a civil matter and recommended it should not be placed in this bill (single Subject)

Makes it a crime to use someone else's identity for criminal activity and crime in and of itself.

Addresses use of new technology such as disk recording devices and distribution systems such as computers.

It also includes computer hacking as a crime.

The bill spells out the severity of the offense based on monetary gain.

Section 1. & 2 are at request. It adds electronic recording to the existing child exploitation laws essentially to match current and hopefully future technology. (Computers, C D's, video and audio disks)

The remainder of the bill defines criminal impersonation and associated crimes.

Section 3. Deals with illegal credit card use or the numbers involved in obtaining credit and establishes its degree of offense.

Section 4. Expands the fraud definition in current statute and establishes the level of the offense based on monetary gain.

Section 5. Adds the offense of obtaining an access device or I.D. either through illegal means or by giving false information.

Section 6. Establishes First degree criminal impersonation (Class B felony)

Section 7. Establishes Second Degree criminal impersonation (Class A Misdemeanor)

Section 8. Adds recording to the definition of business record.

Section 9. Establishes crime level for deceptive business practices done without assistance from a computer. (Class A Misdemeanor)

Section 10. Makes using a computer in the commission of deceptive business practices a Class C felony and defines criminal usage of a computer. (Includes hacking)

Section 11. Hacking- Defines when it is a crime

Section 12-13 Definitions of terms used in the bill.

Section 14 Makes giving false information to a police officer an offense.

Section 15-17 Definitions

Section 18 Applicability and effective date.

1-LS1284K
Luckhaupt
3/20/00

*adopted
3/20/00*

CS FOR SENATE BILL NO. 259(JUD)
IN THE LEGISLATURE OF THE STATE OF ALASKA
TWENTY-FIRST LEGISLATURE - SECOND SESSION

BY THE SENATE JUDICIARY COMMITTEE

Offered:
Referred:

Sponsor(s): SENATOR TAYLOR

A BILL

FOR AN ACT ENTITLED

1 "An Act relating to crimes and offenses relating to aural representations,
2 recordings, access devices, identification documents, impersonation, false reports, and
3 computers; and providing for an effective date."

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

5 * Section 1. AS 11.41.455(a) is amended to read:

6 (a) A person commits the crime of unlawful exploitation of a minor if, in the
7 state and with the intent of producing a live performance, film, audio, video,
8 electronic, or electromagnetic recording, photograph, negative, slide, book,
9 newspaper, magazine, or other [PRINTED] material that visually or aurally depicts
10 the conduct listed in (1) - (7) of this subsection, the person knowingly induces or
11 employs a child under 18 years of age to engage in, or photographs, films, records, or
12 televises a child under 18 years of age engaged in, the following actual or simulated
13 conduct:

14 (1) sexual penetration;

- 1 (2) the lewd touching of another person's genitals, anus, or breast;
2 (3) the lewd touching by another person of the child's genitals, anus,
3 or breast;
4 (4) masturbation;
5 (5) bestiality;
6 (6) the lewd exhibition of the child's genitals; or
7 (7) sexual masochism or sadism.

8 * Sec. 2. AS 11.41.455(b) is amended to read:

9 (b) A parent, legal guardian, or person having custody or control of a child
10 under 18 years of age commits the crime of unlawful exploitation of a minor if, in the
11 state, the person permits the child to engage in conduct described in (a) of this section
12 knowing that the conduct is intended to be used in producing a live performance, film,
13 audio, video, electronic, or electromagnetic recording, photograph, negative, slide,
14 book, newspaper, magazine, or other [PRINTED] material that visually or aurally
15 depicts the conduct.

16 * Sec. 3. AS 11.46.140(a) is amended to read:

17 (a) A person commits the crime of theft in the third degree if the person
18 commits theft as defined in AS 11.46.100 and

19 (1) the value of the property or services is \$50 or more but less than
20 \$500;

21 (2) the property is an access device [A CREDIT CARD]; or

22 (3) the value of the property is less than \$50 and, within the past five
23 years, the person has been convicted and sentenced on two or more separate occasions
24 in this or another jurisdiction of theft or concealment of merchandise, or an offense
25 under another law or ordinance with similar elements.

26 * Sec. 4. AS 11.46.285 is amended to read:

27 Sec. 11.46.285. Fraudulent use of an access device [A CREDIT CARD].

28 (a) A person commits the crime of fraudulent use of an access device [A CREDIT
29 CARD] if, with intent to defraud, the person uses an access device [A CREDIT
30 CARD] to obtain property or services with knowledge that

31 (1) the access device [CARD] is stolen or forged;

1 (2) the access device [CARD] is expired or has been revoked or
2 cancelled; or

3 (3) for any other reason, that person's use of the access device [CARD]
4 is unauthorized by either the issuer or the person to whom the access device [CREDIT
5 CARD] is issued.

6 (b) Fraudulent use of an access device [A CREDIT CARD] is

7 (1) a class B felony if the value of the property or services obtained
8 is \$25,000 or more;

9 (2) a class C felony if the value of the property or services obtained is
10 \$500 or more but less than \$25,000;

11 (3) [(2)] a class A misdemeanor if the value of the property or services
12 obtained is \$50 or more but less than \$500;

13 (4) [(3)] a class B misdemeanor if the value of the property or services
14 obtained is less than \$50.

15 * Sec. 5. AS 11.46.290 is amended to read:

16 Sec. 11.46.290. Obtaining an access device or identification document [A
17 CREDIT CARD] by fraudulent means. (a) A person commits the crime of
18 obtaining an access device or identification document [A CREDIT CARD] by
19 fraudulent means if

20 (1) the person buys an access device or identification document [A
21 CREDIT CARD] from a person other than the issuer or, as other than the issuer, the
22 person sells an access device or identification document [A CREDIT CARD];

23 (2) with intent to defraud, the person obtains an access device or
24 identification document [CONTROL OF A CREDIT CARD AS A SECURITY FOR
25 DEBT]; or

26 (3) with intent to defraud, the person makes a false statement in an
27 application for an access device or identification document [A CREDIT CARD].

28 (b) [OBTAINING A CREDIT CARD BY FRAUDULENT MEANS UNDER
29 (a)(1) OR (2) OF THIS SECTION IS A CLASS C FELONY.] Obtaining an access
30 device or identification document [A CREDIT CARD] by fraudulent means [UNDER
31 (a)(3) OF THIS SECTION] is a class A misdemeanor.

1 * Sec. 6. AS 11.46 is amended by adding a new section to read:

2 Sec. 11.46.565. **Criminal impersonation in the first degree.** (a) A person
3 commits the crime of criminal impersonation in the first degree if the person

4 (1) possesses an access device or identification document of another
5 person;

6 (2) without authorization of the other person, uses the access device or
7 identification document of another person to obtain a false identification document,
8 open an account at a financial institution, obtain an access device, or obtain property
9 or services; and

10 (3) with criminal negligence, damages the financial reputation of the
11 other person.

12 (b) Criminal impersonation in the first degree is a class B felony.

13 * Sec. 7. AS 11.46.570 is amended to read:

14 Sec. 11.46.570. **Criminal impersonation in the second degree.** (a) A person
15 commits the crime of criminal impersonation in the second degree if the person

16 (1) assumes a false identity and does an act in the assumed character
17 with intent to defraud, commit a crime, or obtain a benefit to which the person is
18 not entitled; or

19 (2) pretends to be a representative of some person or organization and
20 does an act in the pretended capacity with intent to defraud, commit a crime, or
21 obtain a benefit to which the person is not entitled.

22 (b) Criminal impersonation in the second degree is a class A misdemeanor.

23 * Sec. 8. AS 11.46.630(b)(1) is amended to read:

24 (1) "business record" means a writing, recording, or article kept or
25 maintained by an enterprise for the purpose of evidencing or reflecting its condition
26 or activity;

27 * Sec. 9. AS 11.46.710(c) is amended to read:

28 (c) Except as provided in (d) of this section, deceptive [DECEPTIVE]
29 business practices is a class A misdemeanor.

30 * Sec. 10. AS 11.46.710 is amended by adding a new subsection to read:

31 (d) Deceptive business practices is a class C felony if the person uses the

1 internet or a computer network to commit the offense. In this subsection, "Internet"
2 means the combination of computer systems or networks that make up the international
3 network for interactive communications services, including remote logins, file transfer,
4 electronic mail, and newsgroups.

5 * Sec. 11. AS 11.46.740(a) is amended to read:

6 (a) A person commits the offense of criminal use of a computer if, having no
7 right to do so or any reasonable ground to believe the person has such a right, the
8 person knowingly accesses, [OR] causes to be accessed, or exceeds the person's
9 authorized access to a computer, computer system, computer program, computer
10 network, or any part of a computer system or network, and, as a result of or in the
11 course of that access,

12 (1) obtains information concerning a person; [OR]

13 (2) introduces false information into a computer, computer system,
14 computer program, or computer network with the intent to damage or enhance the
15 data record or the financial reputation of a person;

16 (3) introduces false information into a computer, computer system,
17 computer program, or computer network and, with criminal negligence, damages
18 or enhances the data record or the financial reputation of a person;

19 (4) obtains proprietary information of another person;

20 (5) obtains information that is only available to the public for a fee;

21 (6) introduces instructions, a computer program, or other
22 information that tampers with, disrupts, disables, or destroys a computer,
23 computer system, computer program, computer network, or any part of a
24 computer system or network; or

25 (7) encrypts or decrypts data.

26 * Sec. 12. AS 11.46.740 is amended by adding a new subsection to read:

27 (c) In this section, "proprietary information" means scientific, technical, or
28 commercial information, including a design, process, procedure, customer list, supplier
29 list, or customer records that the holder of the information has not made available to
30 the public.

31 * Sec. 13. AS 11.46.990 is amended by adding a new paragraph to read:

1 (14) "financial reputation" means a person's

2 (A) ability to obtain a loan from a financial institution, open an
3 account with a financial institution, obtain property or services on credit, or
4 obtain an access device; or

5 (B) creditworthiness in a credit report.

6 * Sec. 14. AS 11.56.800(a) is amended to read:

7 (a) A person commits the crime of making a false report if the person
8 knowingly

9 (1) gives false information to a peace officer with the intent of
10 implicating another in an offense [A CRIME];

11 (2) makes a false report to a peace officer that a crime has occurred or
12 is about to occur;

13 (3) makes a false report or gives a false alarm that a fire or other
14 incident dangerous to life or property calling for an emergency response has occurred
15 or is about to occur; or

16 (4) makes a false report to the Department of Natural Resources under
17 AS 46.17 concerning the condition of a dam or reservoir.

18 * Sec. 15. AS 11.61.125(d) is amended to read:

19 (d) In this section, "distribution" includes delivering, selling, renting, leasing,
20 lending, giving, circulating, exhibiting, presenting, providing, [AND] exchanging, and
21 placing on a computer network or computer system, whether or not for monetary
22 or other consideration.

23 * Sec. 16. AS 11.81.900(b)(48) is amended to read:

24 (48) "property" means an article, substance, or thing of value, including
25 money, tangible and intangible personal property including data or information stored
26 in a computer program, system, or network, real property, an access device [A
27 CREDIT CARD], a domestic pet or livestock regardless of value, choses-in-action, and
28 evidence of debt or of contract; a commodity of a public utility such as gas, electricity,
29 steam, or water constitutes property, but the supplying of such a commodity to
30 premises from an outside source by means of wires, pipes, conduits, or other
31 equipment is considered a rendition of a service rather than a sale or delivery of

1 property;

2 * Sec. 17. AS 11.81.900(b) is amended by adding new paragraphs to read:

3 (61) "access device" means a card, credit card, plate, code, account
4 number, algorithm, or identification number, including a social security number,
5 electronic serial number, or password, that is capable of being used, alone or in
6 conjunction with another access device or identification document, to obtain property
7 or services, or that can be used to initiate a transfer of property;

8 (62) "identification document" means a paper, instrument, or other
9 article used to establish the identity of a person; "identification document" includes a
10 social security card, driver's license, non-driver's identification, birth certificate,
11 passport, employee identification, or hunting or fishing license.

12 * Sec. 18. The uncodified law of the State of Alaska is amended by adding a new section
13 to read:

14 APPLICABILITY. This Act applies to acts and offenses committed or completed on
15 or after the effective date of this Act.

16 * Sec. 19. This Act takes effect immediately under AS 01.10.070(c).

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. CSSB 259 (JUD)

Revision Date/Time (Note if correction) 21-Mar-00 Dept. Affected Administration
 Title "An Act relating to criminal impersonation" BRU Legal and Advocacy Services
 Component Public Defender Agency
 Sponsor Senator Taylor
 Requester (S) JUD Component No. 1631

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services	46.5	46.5	46.5	46.5	46.5	46.5
Travel	3.5	3.5	3.5	3.5	3.5	3.5
Contractual	26.3	26.3	26.3	26.3	26.3	26.3
Supplies	1.9	1.9	1.9	1.9	1.9	1.9
Equipment	6.5	0.0	0.0	0.0	0.0	0.0
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	84.7	78.2	78.2	78.2	78.2	78.2

CAPITAL EXPENDITURES						
----------------------	--	--	--	--	--	--

CHANGE IN REVENUES ()						
------------------------	--	--	--	--	--	--

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF	84.7	78.2	78.2	78.2	78.2	78.2
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	84.7	78.2	78.2	78.2	78.2	78.2

Estimate of any current year (FY2000) cost: _____

POSITIONS

Full-time	1	1	1	1	1	1
Part-time						
Temporary						

ANALYSIS: (Attach a separate page if necessary)

This bill amends current law and adds new statutes to enable prosecution of a wide variety of computer-related offenses.

Prosecution and defense of these offenses will require sophisticated technical expertise. The Public Defender Agency does not currently have staff who have the technical knowledge necessary to defend criminal cases that could be brought under this new legislation.

The Public Defender Agency will need to hire a Programmer Analyst I in order to consult with and train the attorneys appointed to defend these cases. The Programmer Analyst will be based in Anchorage. In addition to providing technical assistance on individual cases in Anchorage, the Programmer Analyst would also be responsible for training attorneys and investigators in all Public Defender Agency offices on technical issues in these cases. One-time equipment costs for computer equipment is also included in the first year.

Prepared by: Barbara Brink, Director Phone 264-4414
 Division Public Defender Agency Date/Time _____
 Approved by Commissioner -- Robert Poe, Jr. Date 3/21/00
 Agency Department of Administration

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. CSSB 259 (JUD)

Revision Date/Time (Note if correction) _____	Dept. Affected <u>Law</u>
Title <u>"An Ac. relating to crimes and offenses relating to aural representations, ... access devices ... computers; ..."</u>	BRU <u>Criminal Division</u>
Sponsor <u>Senator Taylor</u>	Component <u>1st Judicial Dist; 4th Judicial Dist; Criminal Appeals/Special Litigation</u>
Requester <u>Senate Judiciary Committee</u>	Component No. <u>2198;2201;2203</u>

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel	3.3	3.3	3.3	3.3	3.3	3.3
Contractual	6.7	6.7	6.7	6.7	6.7	6.7
Supplier						
Equipm	5.0	5.0	5.0	5.0	5.0	5.0
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	15.0	15.0	15.0	15.0	15.0	15.0

CAPITAL EXPENDITURES						
-----------------------------	--	--	--	--	--	--

CHANGE IN REVENUES ()						
-------------------------------	--	--	--	--	--	--

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF	15.0	15.0	15.0	15.0	15.0	15.0
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	15.0	15.0	15.0	15.0	15.0	15.0

Estimate of any current year (FY2000) cost: _____

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: (Attach a separate page if necessary)

CSSB 259 (JUD) amends and expands the substantive criminal law to address the use of computers and other technology in the widespread perpetration of crimes. Child pornography, theft of personal information with the intent to defraud, theft of personal information resulting in damage to a person's financial reputation, deceptive business practices, "hacking" to get unauthorized information or introduce false information, and introducing damaging viruses, are all offenses where technology has offered new ways for criminals to victimize individuals. The amendments in this bill will update existing law to help law enforcement prosecute those who cause harm to others through the use of computers and other technology.

Prepared by: <u>Joan M. Kasson</u> <i>Joan M. Kasson</i>	Phone <u>465-5370</u>
Division <u>Attorney General's Office</u>	Date/Time <u>3/21/00, 11:39 AM</u>
Approved by <u>Commissioner</u> <i>Hedley</i> <u>Bruce M. Botelho, Attorney General</u>	Date <u>3/21/00</u>
Agency <u>Department of Law</u>	

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. CSSB 259 (JUD)

ANALYSIS CONTINUATION

Much of the bill expands on existing crimes already being prosecuted, and is not anticipated to cause increased workload. The new crimes defined in the bill are expected to result in approximately ten new prosecutions in the first year, with the number increasing in future years. These new white-collar cases will be handled by existing staff. Although no new personnel are believed to be necessary, other resources will be needed.

Investigation and prosecution of cybercrimes require that the prosecutor keep up with the constantly changing world of information technology. Those who use computers to commit crimes are very knowledgeable about technology, and usually have state-of-the-art equipment. Prosecutors must have the same or better knowledge and equipment as those who use the equipment for illegal purposes.

The Department of Law intends to have three of its prosecutors specialize in this technology driven area of law: one in Anchorage OSPA, and one each in the Juneau and Fairbanks district attorney's offices. These assistant district attorneys will need on-going training to stay ahead of the inventive ways people come up with to use technology to cause harm to others and to keep up with how law enforcement is responding in other jurisdictions. The department estimates \$10.0 per year will be spent on training, divided equally between the three components. \$5.0 per year is included to maintain state-of-the-art computer equipment, software, peripherals, and associated communications devices in Anchorage OSPA as a resource for the entire Criminal Division to use in preparing and presenting its cases.

Library References

- Jury instructions, vehicle prowling, . Elements, see Wash.Prac. vol. 11,
 Definition, see Wash.Prac. vol. 11, WPIC 61.02.
 WFIC 61.01.

Notes of Decisions

1. Vehicle

There was no violation of defendant's right to equal protection of laws when defendant, who broke and entered semitrailer, was convicted of burglary in second degree rather than of lesser offense such as vehicle prowling since semitrailer was not a motor vehicle. *State v. Tyson* (1983) 33 Wash.App. 859, 658 P.2d 55.

Person who broke and entered semi trailer could be convicted of burglary in

the second degree, a class B felony; charges were not required to be brought under statutes defining lesser offenses such as vehicle prowling (this section and §§ 9A.04.110 and 46.04.320) since semitrailer is a separate detachable container or structure from truck tractor unit which is used to draw it. *State v. Tyson* (1983) 33 Wash.App. 859, 658 P.2d 55.

9A.52.110. Computer trespass in the first degree

(1) A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system or electronic data base of another; and

(a) The access is made with the intent to commit another crime; or

(b) The violation involves a computer or data base maintained by a government agency.

(2) Computer trespass in the first degree is a class C felony. Enacted by Laws 1984, ch. 273, § 1.

Notes of Decisions

Authorization 2
 Evidence 1

college coeds which were in no way connected to any ongoing police investigation. *State v. Olson* (1987) 47 Wash.App. 514, 735 P.2d 1362.

1. Evidence

Evidence showed at most unauthorized use of computer data, which was not prohibited by this section, and was insufficient to sustain conviction for computer trespass; defendant, a university police officer who had an access code and permission to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of computer, was found retrieving computer printouts of

2. Authorization

Trial court was required to find lack of authorization to use computer beyond a reasonable doubt after independently reviewing evidence in prosecution for computer trespass, and it committed error when it relied on pretrial order to find lack of authority to access computer. *State v. Olson* (1987) 47 Wash.App. 514, 735 P.2d 1362.

9A.52.120. Computer trespass in the second degree

(1) A person is guilty of computer trespass in the second degree if the person, without authorization, intentionally gains access to a

HINGTON CRIMINAL CODE

References

Elements, see Wash.Prac. vol. 11, WPIC 61.02.

Definitions

In the second degree, a class B felony; targets were not required to be brought under statutes defining lesser offenses such as vehicle prowling (this section and §§ 9A.04.110 and 46.04.320) since a trailer is a separate detachable container or structure from truck tractor unit which is used to draw it. State v. Olson (1983) 33 Wash.App. 859, 658 P.2d

In the first degree

Computer trespass in the first degree if intentionally gains access to a computer system or data base of another; and intent to commit another crime;

computer system or data base maintained by another person;

Computer trespass in the first degree is a class C felony.

Definitions

Illegally obtained records which were in no way connected to any ongoing police investigation. State v. Olson (1987) 47 Wash.App. 14, 735 P.2d 1362.

Authorization

Trial court was required to find lack of authorization to use computer beyond reasonable doubt after independently reviewing evidence in prosecution for computer trespass, and it committed error when it relied on pretrial order to find lack of authority to access computer. State v. Olson (1987) 47 Wash.App. 14, 735 P.2d 1362.

In the second degree

Computer trespass in the second degree if intentionally gains access to a

BURGLARY AND TRESPASS

9A.52.130

computer system or electronic data base of another under circumstances not constituting the offense in the first degree.

(2) Computer trespass in the second degree is a gross misdemeanor.

Enacted by Laws 1984, ch. 273, § 2.

9A.52.130. Computer trespass—Commission of other crime

A person who, in the commission of a computer trespass, commits any other crime may be punished for that other crime as well as for the computer trespass and may be prosecuted for each crime separately.

Enacted by Laws 1984, ch. 273, § 3.

Cross References

Physical damage to computer programs, see § 9A.48.100.

BBERY

drafts.
 ermission.

rented machinery, equipment,

efinition—Access devices, pre-

ic first degree.
 ic second degree.
 ic third degree.
 e.

is.
 n services.
 rice used to commit violation.

er.

ic
 ws 1959, ch. 229, §§ 1, 2.
 ws 1961, ch. 63, § 1.
 ws 1965, ch. 32, § 1.
 ws 1967, ch. 76, § 1.
 ws 1975, 1st Ex.Sess., ch. 61, §§ 1, 2.

c Research

ic of Washington Annotated and
 a citation in INSTA-CITE for

THEFT AND ROBBERY

9A.56.010

display of any parallel citations and case history. Enter a constitution, statute or rule citation in a case law database for cases of interest.

Example query for INSTA-CITE: IC 692 P.2d 874

Example query for Washington Constitution:

Const. Constitution /s 8 +3 5

Example query for statute: 59.12.030

Also, see the WESTLAW guide following the Preface pages of this volume.

9A.56.010. Definitions

The following definitions are applicable in this chapter unless the context otherwise requires:

(1) "Appropriate lost or misdelivered property or services" means obtaining or exerting control over the property or services of another which the actor knows to have been lost or mislaid, or to have been delivered under a mistake as to identity of the recipient or as to the nature or amount of the property;

(2) "By color or aid of deception" means that the deception operated to bring about the obtaining of the property or services; it is not necessary that deception be the sole means of obtaining the property or services;

(3) "Access device" means any card, plate, code, account number, or other means of account access that can be used alone or in conjunction with another access device to obtain money, goods, services, or anything else of value, or that can be used to initiate a transfer of funds, other than a transfer originated solely by paper instrument;

(4) "Deception" occurs when an actor knowingly:

(a) Creates or confirms another's false impression which the actor knows to be false; or

(b) Fails to correct another's impression which the actor previously has created or confirmed; or

(c) Prevents another from acquiring information material to the disposition of the property involved; or

(d) Transfers or encumbers property without disclosing a lien, adverse claim, or other legal impediment to the enjoyment of the property, whether that impediment is or is not valid, or is or is not a matter of official record; or

(e) Promises performance which the actor does not intend to perform or knows will not be performed.

9A.56.040. Theft in the second degree

(1) A person is guilty of theft in the second degree if he commits theft of:

--(a) Property or services which exceed(s) two hundred and fifty dollars in value, but does not exceed one thousand five hundred dollars in value; or

(b) A public record, writing, or instrument kept, filed, or deposited according to law with or in the keeping of any public office or public servant; or

(c) An access device; or

(d) A motor vehicle, of a value less than one thousand five hundred dollars; or

(e) A firearm, of a value less than one thousand five hundred dollars.

(2) Theft in the second degree is a class C felony.

Enacted by Laws 1975, 1st Ex.Sess., ch. 260, § 9A.56.040. Amended by Laws 1982, 1st Ex.Sess., ch. 47, § 15; Laws 1987, ch. 140, § 2.

Historical Note

Laws 1982, 1st Ex.Sess., ch. 47, § 15, inserted subsec. (1)(c).

Laws 1987, ch. 140, § 2, rewrote subsec. (1)(c), which previously read: "A credit-card; or".

Severability—Laws 1982, 1st Ex. Sess., ch. 47: See Historical Note following § 9.41.190.

Source:

Laws 1909, ch. 249, § 353.

RRS § 2605.

Former §§ 9.27.030, 9.54.090.

Laws 1955, ch. 97, § 1.

Laws 1963, ch. 133, § 1.

Former § 9.61.220.

Laws 1970, Ex.Sess., ch. 36, § 3.

Cross References

Civil action for shoplifting by adults, minors, see § 4.24.230.

Larceny, see ch. 9.54.

Library References

Criminal Law ¶27.

Larceny ¶5, 24.

C.J.S. Criminal Law § 5 et seq.

C.J.S. Larceny §§ 2 et seq., 66 et seq.

C.J.S. Motor Vehicles § 588.

Criminal practice, disposition without trial, reduction of charge, see Wash.

Prac. vol. 13, Ferguson, § 3014.

Jury instructions, theft, second degree,

Definition, see Wash.Prac. vol. 11, WPIC 70.05.

Elements, see Wash.Prac. vol. 11, WPIC 70.06.

WESTLAW Electronic Research

See WESTLAW guide following the Preface of this volume.

4. Knowledge or intent

Act is done "knowingly," for purposes of statute prohibiting fraud and related activity in connection with identification documents, if it is done voluntarily and intentionally rather than by mistake, accident or other innocent reason. *U.S. v. Smith, D.Or.1988, 685 F.Supp. 1623*, affirmed in part, reversed in part 876 F.2d 898, certiorari denied 110 S.Ct. 194, 493 U.S. 869, 107 L.Ed.2d 149.

4a. Unlawfulness of intended use

Parole violation is a violation of New York law, and thus defendant's alleged unlawful use of identification, which constituted parole violation, could establish element of intent to use "unlawfully" in charge of knowingly possessing with intent to use unlawfully five or more identification documents. *U.S. v. Chandler, C.A.2 (N.Y.) 1998, 98 F.3d 711.*

To enable jury to conclude that defendant intended to use false identifications unlawfully, as required to convict defendant for knowingly possessing with intent to use unlawfully five or more false identification documents, government is required to establish uses to which defendant intended to put false identifications and that those intended uses would violate one or more federal, state, or local laws. *U.S. v. Rohn, C.A.4 (Md.) 1992, 964 F.2d 310.*

5. Identification documents

Defendant may be convicted of using false identification document with intent to defraud United States, within meaning of federal criminal statute, though defendant's conduct does not violate local, state or federal law; violation of such law is not necessary element of statutory offense. *U.S. v. McCormick, C.A.9 (Nev.) 1995, 72 F.3d 1404.*

Nonimmigrant visa was not identification document under statute barring possession of instruments that can be used to make false identification documents; visa only identifies someone as eligible to enter United States without identifying bearer. *U.S. v. Harunouds, C.A.D.C.1995, 51 F.3d 288, 311 U.S.App.D.C. 145*, certiorari denied 116 S.Ct. 2290, 516 U.S. 1128, 132 L.Ed.2d 291.

Possession of credentials appearing to be those of Drug Enforcement Administration (DEA) supported conviction on false credentials charge, even if identification document was contained in leather cover bearing defunct agency's seal and even if statute required that identification document purport to be that of existing agency. *U.S. v. Canan, C.A.6 (Ky.) 1995, 49 F.3d 954*, rehearing and suggestion for rehearing en banc denied, certiorari denied 116 S.Ct. 716, 516 U.S. 1050, 133 L.Ed.2d 670.

For purposes of statute prohibiting fraud and related activity in connection with identification documents, "identification document" is an authentic or real document issued by some governmental body and a "false identification document" is *inter alia* a document procured by false statements or fraud and also may be a non-authentic document. *U.S. v. Smith, D.Or.1988, 685 F.Supp. 1623*, affirmed in part, reversed in part on other grounds 876 F.2d 898, certiorari denied 110 S.Ct. 194, 493 U.S. 869, 107 L.Ed.2d 149.

6. Possession of document-making implements

Evidence that defendants possessed various document-making implements, which were made in other states and countries, and possessed identification cards from three other states was sufficient to establish that unlawful activity was "in or affecting interstate commerce," for purpose of conviction for violating statute which prohibited fraud in connection with identification documents. *U.S. v. Pearce, C.A.4 (N.C.) 1995, 65 F.3d 22.*

Defendant violated statute prohibiting fraud and related activity in connection with identification documents, by possessing document-making implements which would be used in production of false identification document by possessing Texas seal, two blank Rhode Island birth certificates, blank New Jersey driver's license, two blank Social Security cards and blank chauffeur's license form, and by possessing identification document that appeared to be identification document of United States which was stolen or produced without authority knowing that such document was stolen or produced without authority by her possession of blank Social Security card. *U.S. v. Smith, D.Or.1988, 685 F.Supp. 1623*, affirmed in part, reversed in part 876 F.2d 898, certiorari denied 110 S.Ct. 194, 493 U.S. 869, 107 L.Ed.2d 149.

7. Instructions

General unanimity charge instructing jury that it had to return unanimous verdict was sufficient with respect to charge of knowingly possessing and using false identification documents; trial court was not required to provide specific unanimity charge that all jurors had to agree on particular theory of how defendant violated law. *U.S. v. Chandler, C.A.2 (N.Y.) 1996, 98 F.3d 711.*

Defendant was not entitled to venue instruction in prosecution for unlawful production and transfer of false identification documents, as defendant did not interpose question in timely fashion; any asserted defects in venue were apparent to defendant at time defendant entered into stipulation that waived venue issue. *U.S. v. Sotton, C.A.2 (N.Y.) 1994, 13 F.3d 666.*

In prosecution for knowingly possessing with intent to use unlawfully five or more false identification documents, citation to jury of particular law which defendant's intended use of false identification documents would have violated was required; unlawfulness was determined not by reference to abstract notions of right and wrong, but by standards prescribed by appropriate lawmaking bodies, and to demonstrate un-

lawfulness, jury had to be instructed that particular conduct would have violated specific law. *U.S. v. Rahn, C.A.4 (Md.) 1992, 964 F.2d 310.*

8. Weight and sufficiency of evidence

Evidence that defendant possessed 108 counterfeit birth certificates, which he transported from Peru to the United States, that he secreted certificates in newspaper, and that he knew certificates could be used unlawfully to obtain driver's licenses, which produced \$200-\$300 per certificate, was sufficient to establish that defendant had willful intent to transfer certificates unlawfully, to support conviction of possession with intent to transfer unlawfully five or more false identification documents, considering additionally defendant's false exculpatory statements at time of arrest and his discredited claim that he was working for FBI. *U.S. v. Alejandro, C.A.11 (Fla.) 1997, 118 F.3d 1513.*

Evidence that both defendants had constructive, if not actual, possession of residence and rental car in which document-making implements were found was sufficient to sustain convictions for violating statute which prohibited fraud in connection with identification documents. *U.S. v. Pearce, C.A.4 (N.C.) 1995, 65 F.3d 22.*

Government's proposed inference that defendant intended unlawful uses of multiple false identification documents which she possessed as there were no possible lawful uses for false identifications was not sufficient to establish that defendant's intended uses of false identifications would violate federal, state, or local laws, so as to permit conviction for knowingly possessing with intent to use unlawfully five or more false identification documents. *U.S. v. Rohn, C.A.4 (Md.) 1992, 964 F.2d 310.*

9. Admissibility of evidence

Any "Oriental prejudice" suffered by defendant charged under federal statute with making false identification cards as result of evidence that defendant's activities violated Illinois law as well as federal law did not require mistrial, where any prejudice was outweighed by probative value of state employee's testimony on element of government's case. *U.S. v. Bell, C.A.7 (Ill.) 1997, 980 F.2d 1096.*

10. Discipline of attorneys

One-year suspension is appropriate sanction for attorney who is convicted of aiding and abetting in possession and use of identification document in order to fraudulently obtain passport, not involving moral turpitude. *In re McBride, D.C.1994, 642 A.2d 1270.*

§ 1029. Fraud and related activity in connection with access devices

(a) Whoever—

- (1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
- (2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period;
- (3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than \$1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) Penalties.—

(1) Generally.—The punishment for an offense under subsection (a) of this section is.—

(A) in the case of an offense that does not occur after a conviction for another offense under this section.—

(i) If the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii) If the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years; or both;

(B) in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

(C) in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

(2) Forfeiture procedure.—The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

tent to defraud, produces, traffics in, has control or making equipment;

tent to defraud effects transactions with 1 or more person or persons, to receive payment or any other ar period the aggregate value of which is equal to or

on of the issuer of the access device, knowingly and a person for the purpose of— device; or

n regarding or an application to obtain an access

ent to defraud uses, produces, traffics in, has control telecommunication instrument that has been modified zed use of telecommunications services;

ent to defraud uses, produces, traffics in, has control scanning receiver;

es, traffics in, has control or custody of, or possesses ng it has been configured to insert or modify telecom- ation associated with or contained in a telecommunica- instrument may be used to obtain telecommunications or

tion of the credit card system member or its agent, o defraud causes or arranges for another person to agent, for payment, 1 or more evidences or records of as device;

tate or foreign commerce, be punished as provided in

submit an offense under subsection (a) of this section alties as those prescribed for the offense attempted.

spiracy of two or more persons to commit an offense ion, if any of the parties engages in any conduct in ll be fined an amount not greater than the amount r such offense under subsection (c) of this section or alf the period provided as the maximum imprisonment (c) of this section, or both.

ishment for an offense under subsection (a) of this

n offense that does not occur after a conviction for ds section.

is under paragraph (1), (2), (3), (6), (7), or (10) of e under this title or imprisonment for not more than 10

is under paragraph (4), (5), (8), or (9), of subsection (a), le or imprisonment for not more than 15 years, or both;

n offense that occurs after a conviction for another n, a fine under this title or imprisonment for not more and

refture to the United States of any personal property sed to commit the offense.

—The forfeiture of property under this section, includ- ion of the property and any related administrative and governed by section 413 of the Controlled Substances) of that section.

Service shall, in addition to any other agency having ty to investigate offenses under this section. Such cret Service shall be exercised in accordance with an red into by the Secretary of the Treasury and the

(e) As used in this section—

(1) the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument);

(2) the term "counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device;

(3) the term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud;

(4) the term "produce" includes design, alter, authenticate, duplicate, or assemble;

(5) the term "traffic" means transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of;

(6) the term "device-making equipment" means any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device;

(7) The term "credit card system member" means a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system;

(8) the term "scanning receiver" means a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument

(9) the term "telecommunications service" has the meaning given such term in section 3 of title I of the Communications Act of 1934 (47 U.S.C. 163);

(10) the term "facilities-based carrier" means an entity that owns communica- tions transmission facilities, is responsible for the operation and maintenance of those facilities, and holds an operating license issued by the Federal Communica- tions Commission under the authority of title III of the Communications Act of 1934; and

(11) the term "telecommunication identifying information" means electronic seri- al number or any other number or signal that identifies a specific telecommunica- tions instrument or account, or a specific communication transmitted from a telecommunications instrument.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title. For purposes of this subsection, the term "State" includes a State of the United States, the District of Columbia, and any commonwealth, territory, or possession of the United States.

(g)(1) It is not a violation of subsection (a)(9) for an officer, employee, or agent of, or a person engaged in business with, a facilities-based carrier, to engage in conduct (other than trafficking) otherwise prohibited by that subsection for the purpose of protecting the property or legal rights of that carrier, unless such conduct is for the purpose of obtaining telecommunications service provided by another facilities-based carrier, with- out the authorization of such carrier.

(2) In a prosecution for a violation of subsection (a)(9), (other than a violation consisting of producing or trafficking) it is an affirmative defense (which the defendant must establish by a preponderance of the evidence) that the conduct charged was engaged in for research or development in connection with a lawful purpose.

(Added Pub.L. 98-473, Title II, § 1602(a), Oct. 12, 1984, 98 Stat. 2183, and amended Pub.L. 99-646, § 44(b), Nov. 10, 1986, 100 Stat. 3601; Pub.L. 101-647, Title XII, § 1206(f), Nov. 29, 1990, 104 Stat. 4831; Pub.L. 103-222, Title XXV, § 250007, Title XXXIII, § 330016(c)(1), Sept. 18, 1994, 108 Stat. 2087, 2148; Pub.L. 103-414, Title II, § 206, Oct. 26, 1994, 108 Stat. 4291; Pub.L. 104-294, Title VI, § 601(d), Oct. 11, 1996, 110 Stat. 3601; Pub.L. 105-172, § 2(a) - (d), Apr. 24, 1998, 112 Stat. 63.)

Note 16

relate to sufficiency of the evidence, but rather to manner in which defendant was charged. *U.S. v. Akpl*, C.A.4 (Md.) 1994, 28 F.3d 24.

17. Questions of fact

Evidence presented jury question as to whether defendant was guilty, either as aider and abettor or as principal, of bank fraud and access device fraud; with respect to direct use of access device, at least one automatic teller machine (ATM) photograph showed defendant in driver's seat of vehicle parked at drive-through ATM, and defendant was pictured with codefendant as another card was being used, which suggested that he knew of and did nothing to prevent the crime. *U.S. v. Padayini*, C.A.D.C.1994, 28 F.3d 1238, 307 U.S.App.D.C. 369, rehearing denied.

18. Cloned cellular telephones

Defendant's cellular telephone cloning activities, involving use of electronic scanning and computer programming equipment to erase and reprogram electronic chip containing cellular phone's electronic serial number and mobile identification number with account number of another user, so that calls made on modified phone would be charged to other user's account, violated statute prohibiting knowing possession, production, use, and trafficking of counterfeit access devices and access device equipment, even before statute was amended to specifically address cellular telephone cloning. *U.S. v. Watson*, C.A.9 (Cal.) 1997, 118 F.3d 1916.

Cloned cellular telephone, i.e., one with identification numbers identical to another existing legitimate unit, fell within ambit of federal statute governing fraud and related activity in connection with access devices, in prosecution for violations of statute arising from defendant's alleged use, possession, and trafficking of cloned cellular telephone; defendant's conduct involved use of altered telecommunications instrument to obtain access to telecommunications services for purpose of defrauding carrier, and cellular carriers were damaged since, by cloning of cellular telephones to enable users to have extension telephone, cellular carriers were defrauded of activation fee and monthly service fee they charged for each cellular telephone. *U.S. v. Yates*, E.D.Ky.1995, 914 F.Supp. 162.

19. Intent

Statute making it illegal to knowingly and with intent to defraud possess 16 or more coun-

terfeit or unauthorized access devices if offense affects interstate commerce requires government to prove only that aggregate possession of 16 or more unauthorized access devices affected interstate commerce does not require government to prove intent to defraud with respect to each individual device. *U.S. v. Clayton*, C.A.9 (Cal.) 1997, 108 F.3d 1114, certiorari denied 118 S.Ct. 293, 139 L.Ed.2d 165.

To convict for use of unauthorized access devices, government must prove that defendant acted knowingly and with intent to defraud, but proof of such intent may be established with circumstantial evidence. *U.S. v. Immola*, C.A.5 (Tex.) 1996, 100 F.3d 380, rehearing denied, certiorari denied 117 S.Ct. 1712, 137 L.Ed.2d 836, certiorari denied 117 S.Ct. 1858, 137 L.Ed.2d 1060.

20. Instructions

Defendant charged with possession of cloned cellular phones, cloning equipment, and unauthorized cellular phone identification numbers was not entitled to instruction emphasizing that intent to defraud was necessary element of offenses, as instructions given already listed fraud as element of offense. *U.S. v. Clayton*, C.A.9 (Cal.) 1997, 108 F.3d 1114, certiorari denied 118 S.Ct. 293, 139 L.Ed.2d 165.

21. Value of loss

Court did not err in calculating amount of intended loss through use of fake credit cards at \$2,500,000 by adding the number of completed false cards, unembossed cards, signature panels, other unembossed cards found in safe in hotel where some of defendants were staying and then multiplying by the \$6,900 average amount charged per account during two weeks prior to defendant's arrest. *U.S. v. Wal-Keung*, C.A.11 (Fla.) 1997, 115 F.3d 874, rehearing and suggestion for rehearing en banc denied 127 F.3d 42, certiorari denied 118 S.Ct. 1096, 140 L.Ed.2d 160.

22. Unauthorized device

Merchant account numbers used by defendants in furtherance of bank fraud scheme were "unauthorized" access devices, based on evidence that merchant bank prohibited practice of factoring, by which business would use third party as conduit for depositing credit card sales, and that defendants knew of and intentionally violated bank's policy. *U.S. v. Dabbs*, C.A.11 (Fla.) 1998, 184 F.3d 1071.

§ 1030. Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same

ut rather charged. F.3d 24.

as to as' sider fraud and direct use the teller defendant at drive- red with ing used, did noth- Fadayinl. App.D.C.

terfeit or unauthorized access devices if offense effects interstate commerce requires government to prove only that aggregate possession of 15 or more unauthorized access devices affected interstate commerce does not require government to prove intent to defraud with respect to each individual device. U.S. v. Clayton, C.A.9 (Cal.) 1997, 108 F.3d 1114, certiorari denied 118 S.Ct. 233, 139 L.Ed.2d 165.

To convict for use of unauthorized access devices, government must prove that defendant acted knowingly and with intent to defraud, but proof of such intent may be established with circumstantial evidence. U.S. v. Ismoila, C.A.5 (Tex.) 1990, 100 F.3d 380, rehearing denied, certiorari denied 117 S.Ct. 1712, 137 L.Ed.2d 838, certiorari denied 117 S.Ct. 1858, 137 L.Ed.2d 1060.

20. Instructions

ig activi- ning and trace and cellular mobile number of modified account, session, counterfeit equipment, medically i. v. Wat-

Defendant charged with possession of cloned cellular phones, cloning equipment, and unauthorized cellular phone identification numbers was not entitled to instruction emphasizing that intent to defraud was necessary element of offenses, as instructions given already listed fraud as element of offense. U.S. v. Clayton, C.A.9 (Cal.) 1997, 108 F.3d 1114, certiorari denied 118 S.Ct. 233, 139 L.Ed.2d 165.

21. Value of loss

th identi- existing eral stat- y in con- dition for defendant's of cloned involved ument to vices for lar carri- f cellular extension aided of fee they U.S. v.

Court did not err in calculating amount of intended loss through use of fake credit cards at \$2,500,000 by adding the number of completed false cards, unembossed cards, signature panels, other unembossed cards found in safe in hotel where some of defendants were staying and then multiplying by the \$6,900 average amount charged per account during two weeks prior to defendants' arrest. U.S. v. Wai-Keung, C.A.11 (Fla.) 1997, 115 F.3d 874, rehearing and suggestion for rehearing en banc denied 127 F.3d 42, certiorari denied 118 S.Ct. 1096, 140 L.Ed.2d 160.

22. Unauthorized device

igly and ro coun-

Merchant account numbers used by defendants in furtherance of bank fraud scheme were "unauthorized" access devices, based on evidence that merchant bank prohibited practice of factoring, by which business would use third party as conduit for depositing credit card sales, and that defendants knew of and intentionally violated bank's policy. U.S. v. Dabbe, C.A.11 (Fla.) 1998, 184 F.3d 1771.

ity in connection with computers

sed a computer without authorization or exceeding uses of such conduct having obtained information that United States Government pursuant to an Executive protection against unauthorized disclosure for reasons of national security, or any restricted data, as defined in paragraph 1 of the Energy Act of 1954, with reason to believe that such information willfully communicates, delivers, transmits, or is delivered, or transmitted, or attempts to communicate, deliver, or transmitted, or transmitted the same

to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(C), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

18 § 1030

CRIMES AND CRIMINAL PROCEDURE

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
 (iii) the value of the information obtained exceeds \$5,000;

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

[(4) Repealed. Pub.L. 104-294, Title II, § 201(2)(D), Oct. 11, 1996, 110 Stat. 3493]

(d) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section—

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer—

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means—

(A) an institution with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

CRIMES AND CRIMINAL PROCEDURE

CRIMES AND CRIMINAL PROCEDURE

18 § 1030

itted in furtherance of any criminal or tortious act on or laws of the United States or of any State; or nation obtained exceeds \$5,000;

nprisonment for not more than ten years, or both, subsection (a)(2), (a)(3) or (a)(6) of this section which their offense under this section, or an attempt to lter this subparagraph; and

or imprisonment for not more than five years, or lter subsection (a)(4), (a)(5)(A), (a)(5)(B), or (a)(7) of : after a conviction for another offense under this t an offense punishable under this subparagraph;

nprisonment for not more than ten years, or both, subsection (a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or s after a conviction for another offense under this t an offense punishable under this subparagraph;

34, Title II, § 201(2)(D), Oct. 11, 1996, 110 Stat.

rice shall, in addition to any other agency having i investigate offenses under subsections (a)(2)(A), (6) of this section. Such authority of the United ad in accordance with an agreement which shall be reasury and the Attorney General.

is an electronic, magnetic, optical, electrochemical, essageing device performing logical, arithmetic, or ny data storage facility or communications facility i cc _unction with such device, but such term does iter or typesetter, a portable hand held calculator,

ter" means a computer—

ie of a financial institution or the United States of a computer not exclusively for such use, used by or the United States Government and the conduct ts that use by or for the financial institution or the

state or foreign commerce or communication;

the District of Columbia, the Commonwealth of monwealth, possession or territory of the United

on" means—

osits insured by the Federal Deposit Insurance

or a member of the Federal Reserve including any

accounts insured by the National Credit Union

lteral home loan bank system and any home loan

Farm Credit System under the Farm Credit Act of

ored with the Securities and Exchange Commis- the Securities Exchange Act of 1934;

r Protection Corporation;

of a foreign bank (as such terms are defined in tion 1(b) of the International Banking Act of 1978);

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act.

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of "a 5; and

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information, that—

(A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals;

(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

(C) causes physical injury to any person; or

(D) threatens public health or safety; and

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage, as defined in subsection (e)(8)(A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190, and amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7055, Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 982(a)(6), Aug. 9, 1989, 103 Stat. 502; Pub.L. 101-647, Title XII, § 1205(a), Title XXV, § 2697(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub.L. 103-322, Title XXIX, § 290001(b) to (f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3401, 3508.)

HISTORICAL AND STATUTORY NOTES

References in Text

References to "paragraph y of section 11 of the Atomic Energy Act of 1954", referred to in subsec. (a)(1) is classified to section 2014(y) of Title 42, Public Health and Welfare.

The Fair Credit Reporting Act, referred to in subsec. (a)(2)(A), is Title VI of Pub.L. 90-321 as added by Pub.L. 91-508, Title VI, Oct. 20, 1970, 84 Stat. 1127, which is classified to subchapter III (section 1681 et seq.) of chapter 41 of Title 15, Commerce and Trade.

The Farm Credit Act of 1971, referred to in subsec. (c)(4)(E), is Pub.L. 92-181, Dec. 10, 1971, 85 Stat. 685, as amended, which is classified generally to chapter 23 (section 2001 et seq.) of Title 12, Banks and Banking. For complete classification of this Act to the Code, see Short Title note set out under section 2001 of Title 12 and Tables.

Section 16 of the Securities Exchange Act of 1934, referred to in subsec. (e)(4)(F), is classified to section 78o of Title 15, Commerce and Trade.

Section 1(b) of the International Banking Act of 1978, referred to in subsec. (e)(4)(H), is classified to section 3101 of Title 12, Banks and Banking.

Section 25 of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter I (section 601 et seq.) of chapter 6 of Title 12.

Section 25(a) of the Federal Reserve Act, referred to in subsec. (e)(4)(I), is classified to subchapter II (section 611 et seq.) of chapter 6 of Title 12.

The date of the enactment of this subsection, referred to in subsec. (h), means the date of the enactment of Pub.L. 103-322, 108 Stat. 1796, which enacted subsec. (h) and was approved Sept. 13, 1994.

1-LS1284U
Luckhaupt
3/2/00

*Adopted
3/3/00*

CS FOR SENATE BILL NO. 259(JUD)

IN THE LEGISLATURE OF THE STATE OF ALASKA

TWENTY-FIRST LEGISLATURE - SECOND SESSION

BY THE SENATE JUDICIARY COMMITTEE

Offered:
Referred:

Sponsor(s): SENATOR TAYLOR

A BILL

FOR AN ACT ENTITLED

1 "An Act relating to crimes and offenses relating to aural representations,
2 recordings, access devices, identification documents, impersonation, and computers;
3 and providing for an effective date."

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:

5 * Section 1. AS 11.41.455(a) is amended to read:

6 (a) A person commits the crime of unlawful exploitation of a minor if, in the
7 state and with the intent of producing a live performance, film, audio, video,
8 electronic, or electromagnetic recording, photograph, negative, slide, book,
9 newspaper, magazine, or other [PRINTED] material that visually or aurally depicts
10 the conduct listed in (1) - (7) of this subsection, the person knowingly induces or
11 employs a child under 18 years of age to engage in, or photographs, films, records, or
12 televises a child under 18 years of age engaged in, the following actual or simulated
13 conduct:

14 (1) sexual penetration;

- 1 (2) the lewd touching of another person's genitals, anus, or breast;
- 2 (3) the lewd touching by another person of the child's genitals, anus,
- 3 or breast;
- 4 (4) masturbation;
- 5 (5) bestiality;
- 6 (6) the lewd exhibition of the child's genitals; or
- 7 (7) sexual masochism or sadism.

8 * Sec. 2. AS 11.41.455(b) is amended to read:

9 (b) A parent, legal guardian, or person having custody or control of a child
10 under 18 years of age commits the crime of unlawful exploitation of a minor if, in the
11 state, the person permits the child to engage in conduct described in (a) of this section
12 knowing that the conduct is intended to be used in producing a live performance, film,
13 audio, video, electronic, or electromagnetic recording, photograph, negative, slide,
14 book, newspaper, magazine, or other [PRINTED] material that visually or aurally
15 depicts the conduct.

16 * Sec. 3. AS 11.46.140(a) is amended to read:

17 (a) A person commits the crime of theft in the third degree if the person
18 commits theft as defined in AS 11.46.100 and

- 19 (1) the value of the property or services is \$50 or more but less than
- 20 \$500;
- 21 (2) the property is an access device [A CREDIT CARD]; or
- 22 (3) the value of the property is less than \$50 and, within the past five
- 23 years, the person has been convicted and sentenced on two or more separate occasions
- 24 in this or another jurisdiction of theft or concealment of merchandise, or an offense
- 25 under another law or ordinance with similar elements.

26 * Sec. 4. AS 11.46.285 is amended to read:

27 Sec. 11.46.285. Fraudulent use of an access device [A CREDIT CARD].

28 (a) A person commits the crime of fraudulent use of an access device [A CREDIT
29 CARD] if, with intent to defraud, the person uses an access device [A CREDIT
30 CARD] to obtain property or services with knowledge that

- 31 (1) the access device [CARD] is stolen or forged;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

(2) the access device [CARD] is expired or has been revoked or cancelled; or

(3) for any other reason, that person's use of the access device [CARD] is unauthorized by either the issuer or the person to whom the access device [CREDIT CARD] is issued.

(b) Fraudulent use of an access device [A CREDIT CARD] is

(1) a class B felony if the value of the property or services obtained is \$25,000 or more;

(2) a class C felony if the value of the property or services obtained is \$500 or more but less than \$25,000;

(3) [(2)] a class A misdemeanor if the value of the property or services obtained is \$50 or more but less than \$500;

(4) [(3)] a class B misdemeanor if the value of the property or services obtained is less than \$50.

* Sec. 5. AS 11.46.290 is amended to read:

Sec. 11.46.290. Obtaining an access device or identification document [A CREDIT CARD] by fraudulent means. (a) A person commits the crime of obtaining an access device or identification document [A CREDIT CARD] by fraudulent means if

(1) the person buys an access device or identification document [A CREDIT CARD] from a person other than the issuer or, as other than the issuer, the person sells an access device or identification document [A CREDIT CARD];

(2) with intent to defraud, the person obtains an access device or identification document [CONTROL OF A CREDIT CARD AS A SECURITY FOR DEBT]; or

(3) with intent to defraud, the person makes a false statement in an application for an access device or identification document [A CREDIT CARD].

(b) [OBTAINING A CREDIT CARD BY FRAUDULENT MEANS UNDER (a)(1) OR (2) OF THIS SECTION IS A CLASS C FELONY.] Obtaining an access device or identification document [A CREDIT CARD] by fraudulent means [UNDER (a)(3) OF THIS SECTION] is a class A misdemeanor.

JLD

L

1 * Sec. 6. AS 11.46 is amended by adding a new section to read:

2 **Sec. 11.46.565. Criminal impersonation in the first degree.** (a) A person
3 commits the crime of criminal impersonation in the first degree if the person

4 (1) possesses an access device or identification document of another
5 person;

6 (2) without authorization of the other person, uses the access device or
7 identification document of another person to obtain a false identification document,
8 open an account at a financial institution, obtain an access device, or obtain property
9 or services; and

10 (3) with criminal negligence, damages the financial reputation of the
11 other person.

12 (b) Criminal impersonation in the first degree is a class B felony.

13 * Sec. 7. AS 11.46.570 is amended to read:

14 **Sec. 11.46.570. Criminal impersonation in the second degree.** (a) A person
15 commits the crime of criminal impersonation in the second degree if the person

16 (1) assumes a false identity and does an act in the assumed character
17 with intent to defraud, commit a crime, or obtain a benefit to which the person is
18 not entitled; or

19 (2) pretends to be a representative of some person or organization and
20 does an act in the pretended capacity with intent to defraud, commit a crime, or
21 obtain a benefit to which the person is not entitled.

22 (b) Criminal impersonation in the second degree is a class A misdemeanor.

23 * Sec. 8. AS 11.46.630(b)(1) is amended to read:

24 (1) "business record" means a writing, recording, or article kept or
25 maintained by an enterprise for the purpose of evidencing or reflecting its condition
26 or activity;

27 * Sec. 9. AS 11.46.710(c) is amended to read:

28 (c) Except as provided in (d) of this section, deceptive [DECEPTIVE]
29 business practices is a class A misdemeanor.

30 * Sec. 10. AS 11.46.710 is amended by adding a new subsection to read:

31 (d) Deceptive business practices is a class C felony if the person uses a

1 computer, computer system, computer program, computer network, or any part of a
2 computer system or network to commit the offense.

3 * Sec. 11. AS 11.46.740(a) is amended to read:

4 (a) A person commits the offense of criminal use of a computer if, having no
5 right to do so or any reasonable ground to believe the person has such a right, the
6 person knowingly accesses, [OR] causes to be accessed, or exceeds the person's
7 authorized access to a computer, computer system, computer program, computer
8 network, or any part of a computer system or network, and, as a result of or in the
9 course of that access,

10 (1) obtains information concerning a person; [OR]

*define
or remove* →

11 (2) introduces false or misleading information into a computer,
12 computer system, computer program, or computer network with the intent to damage
13 or enhance the data record or the financial reputation of a person;

14 (3) introduces false or misleading information into a computer,
15 computer system, computer program, or computer network and, with criminal
16 negligence, damages or enhances the data record or the financial reputation of a
17 person;

18 (4) obtains proprietary information of another person;

19 (5) obtains information that is only available to the public for a fee;

20 (6) introduces instructions, a computer program, or other
21 information that tampers with, disrupts, disables, or destroys a computer,
22 computer system, computer program, computer network, or any part of a
23 computer system or network; or

24 (7) encrypts or decrypts data.

25 * Sec. 12. AS 11.46.740 is amended by adding a new subsection to read:

26 (c) In this section, "proprietary information" means scientific, technical, or
27 commercial information, including a design, process, procedure, customer list, supplier
28 list, or customer records that the holder of the information has not made available to
29 the public.

30 * Sec. 13. AS 11.46.990 is amended by adding a new paragraph to read:

31 (14) "financial reputation" means a person's

*To
BRAD*

"or misleading"

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

(A) ability to obtain a loan from a financial institution, open an account with a financial institution, obtain property or services on credit, or obtain an access device; or

(B) creditworthiness in a credit report.

* Sec. 14. AS 11.61.125(d) is amended to read:

(d) In this section, "distribution" includes delivering, selling, renting, leasing, lending, giving, circulating, exhibiting, presenting, providing, [AND] exchanging, and placing on a computer network or computer system, whether or not for monetary or other consideration.

* Sec. 15. AS 11.81.900(b)(48) is amended to read:

(48) "property" means an article, substance, or thing of value, including money, tangible and intangible personal property including data or information stored in a computer program, system, or network, real property, an access device [A CREDIT CARD], a domestic pet or livestock regardless of value, choses-in-action, and evidence of debt or of contract; a commodity of a public utility such as gas, electricity, steam, or water constitutes property, but the supplying of such a commodity to premises from an outside source by means of wires, pipes, conduits, or other equipment is considered a rendition of a service rather than a sale or delivery of property;

* Sec. 16. AS 11.81.900(b) is amended by adding new paragraphs to read:

(61) "access device" means a card, credit card, plate, code, account number, algorithm, or identification number, including a social security number, electronic serial number, or password, that is capable of being used, alone or in conjunction with another access device or identification document, to obtain property or services, or that can be used to initiate a transfer of property;

(62) "identification document" means a paper, instrument, or other article used to establish the identity of a person; "identification document" includes a social security card, driver's license, non-driver's identification, birth certificate, passport, employee identification, or hunting or fishing license.

* Sec. 17. The uncodified law of the State of Alaska is amended by adding a new section to read:

- 1 APPLICABILITY. This Act applies to acts and offenses committed or completed on
- 2 or after the effective date of this Act.
- 3 * Sec. 18. This Act takes effect immediately under AS 01.10.070(c).

LEGAL SERVICES

DIVISION OF LEGAL AND RESEARCH SERVICES
LEGISLATIVE AFFAIRS AGENCY
STATE OF ALASKA

(907) 465-3867 or 465-2450
FAX (907) 465-2029
Mail Stop 3101

State Capitol
Juneau, Alaska 99801-1182
Deliveries to: 129 6th St., Rm. 329

MEMORANDUM

February 28, 2000

SUBJECT: Merging of SB 245 and SB 259 (Work Order No. 21-LS1284/G)

TO: Senator Robin Taylor
Attn: Sue

FROM: Gerald P. Luckhaupt *Jer*
Legislative Counsel

Enclosed is the bill you requested. Under Art. II, § 13, Constitution of the State of Alaska, each "bill shall be confined to one subject. . ." I'm not sure there is a single subject for this bill. Most things in the bill relate to criminal law but the provisions relating to electronic storage in bill sec. 17 reach beyond criminal as do the provisions we have added about consumer credit reporting agencies. We could try to argue that the bill relates to access, transfer, or storage of information, services, or property I guess, but some forms of the access device do not necessarily relate to that. In any event, I haven't had much time to review this so I am merely making you aware that this bill seems rather broad to me.

In addition, the revisor of statutes strongly believes that the bills title does not meet the fair express requirement of the Constitution.

GPL:jdr:glc
00-099:jdr

Enclosure

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. SB 259

Revision Date/Time (Note if correction) _____ Dept. Affected Department of Corrections
 Title "An Act relating to criminal impersonation." BRU Administration and Operations
 Component All
 Sponsor Senator Taylor
 Requester House Judiciary Component No. #0694

Expenditures/Revenues (Thousands of Dollars)

Note: Amounts do not include inflation unless otherwise noted below.

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006
Personal Services						
Travel						
Contractual						
Supplies						
Equipment						
Land & Structures						
Grants & Claims						
Miscellaneous						
TOTAL OPERATING	0.0	0.0	0.0	0.0	0.0	0.0

CAPITAL EXPENDITURES						
----------------------	--	--	--	--	--	--

CHANGE IN REVENUES ()						
------------------------	--	--	--	--	--	--

FUND SOURCE (Thousands of Dollars)

1002 Federal Receipts						
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
Other (Specify Type)						
TOTAL	0.0	0.0	0.0	0.0	0.0	0.0

Estimate of any current year (FY2000) cost: 0.0

POSITIONS

Full-time						
Part-time						
Temporary						

ANALYSIS: (Attach a separate page if necessary)

This bill would broaden the definition for criminal impersonation to include "with the intent to commit a crime". The Department does not anticipate that this will make a significant impact on the number of people incarcerated or their length of incarceration. Therefore, the Department is submitting a zero fiscal note.

Prepared by: Candy Brower, Legislative Liaison Phone 465-3307
 Division Commissioner's Office Date/Time 2/12/00 2:55 PM
 Approved by Commissioner Margaret M. Pugh Date 2-14-00
 Agency Dept. of Corrections

PREPARER TO PROVIDE ALL DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE

For further distribution information, call the Governor's Legislative Office

FISCAL NOTE

STATE OF ALASKA
2000 LEGISLATIVE SESSION

BILL NO. SB 259

Revision Date: February 15, 2000
Title: "An Act relating to criminal impersonation"
Sponsor: Senator Taylor
Requestor: (S) JUD

Department Affected: Administration
BRU: Legal and Advocacy Services
Component: Public Defender Agency
COMPONENT SERIAL NO. 1631

EXPENDITURES/REVENUES: (Thousands of Dollars)

OPERATING EXPENDITURES	FY 2001	FY 2002	FY 2 003	FY 2004	FY 2005	FY 2006
PERSONAL SERVICES	**	**	**	**	**	**
TRAVEL						
CONTRACTUAL						
SUPPLIES						
EQUIPMENT						
LAND & STRUCTURES						
GRANTS, CLAIMS						
MISCELLANEOUS						
TOTAL OPERATING	**	**	**	**	**	**
CAPITAL EXPENDITURES	**	**	**	**	**	**
CHANGE IN REVENUES ()	**	**	**	**	**	**

FUND SOURCE: (Thousands of Dollars)

1002 Federal Receipts	**	**	**	**	**	**
1003 GF Match						
1004 GF						
1005 GF/Program Receipts						
1037 GF/Mental Health						
OTHER						
TOTAL	**	**	**	**	**	**

Estimate of any current year (FY 00) cost: \$ -0-

POSITIONS:

FULL-TIME						
PART-TIME						
TEMPORARY						

ANALYSIS: (Attach a separate page if necessary.)

Prepared by: Barbara Brink, Director
Division: Public Defender Agency

Phone: (907) 264-4414
Date: February 15, 2000

Approved by Commissioner: Robert Poe, Jr. / [Signature]
Agency: Department of Administration

Date: February 15, 2000 2/15/00

DISTRIBUTION COPIES TO GOVERNOR'S LEGISLATIVE OFFICE
For further distribution information, call the Governor's Legislative Office

FISCAL NOTE

STATE OF ALASKA

BILL NO. SB 259

2000 LEGISLATIVE SESSION

ANALYSIS: (continued)

This bill would add a provision to the Criminal Impersonation statute that would make possession of a false identification card or an identification card that belongs to someone else a class A misdemeanor offense. The defendant would have to possess the card with intent to commit a crime or to defraud.

The Public Defender Agency expects some financial impact as a result of this bill. This bill significantly expands the activity covered by criminal impersonation. We estimate that there are many cases where underage people use "false id's" to try to get alcohol and tobacco. If these all these cases end up being prosecuted as state misdemeanors, the impact could be significant. However, with our current information, it is not possible to make an accurate estimate of the number of new cases that will be prosecuted. Therefore, the Public Defender Agency is submitting an indeterminate fiscal note.

SENATE COMMITTEE REPORT

First Committee of Referral

DATE: 2/10/00

FURTHER: Finance

Date of 5-Day Notice: _____
(in accordance with Uniform Rule 23)

DATE TURNED
IN TO OFFICE: _____

Judiciary Committee considered

SENATE BILL NO. 259

"An Act relating to criminal impersonation."

and recommends:

be replaced with _____ CS SP 259 (JUD)

adopt previous _____ CS _____

attached amendment(s)

adopt Letter of Intent by _____ Committee

further referral to the _____ Committee

Senate Bill:

same title
 new title

House Bill:

same title
 technical title
 new: SCR# _____

SIGNING <u>DO</u> PASS	DP	OTHER RECOMMENDATIONS	NR	DNP	AM
		<i>[Signature]</i>	✓		
		<i>[Signature]</i>	X		
		<i>[Signature]</i>	✓		
CHAIR: <i>[Signature]</i>	✓	CHAIR:			

NEW FISCAL NOTE(S):

Department Date Zero Fiscal

CORRECTION	2/14	✓	
ADMINISTRATION	2/15		*
JUDICIAL SAFETY	3/8		145.6

PREVIOUS FISCAL NOTE(S):*

Department Date Zero Fiscal

APPROPRIATION -- no fiscal note

*include fiscal notes accompanying Governor's bill

Impostor gains access to couple's savings

By AMANDA BOHMAN
Staff Writer

When Nancy Kuhn received a letter from her credit union asking to verify her change of address to Juneau, she knew there was a mistake.

The Kuhns, who live in Fairbanks, hadn't moved to Juneau and didn't plan to.

Kuhn called Alaska USA Federal Credit Union to tell them the address change was wrong. That's when she learned of the four withdrawals from her account.

Someone posing as her husband not only changed the address of the account but had most of the money—\$4,900—wired to Georgia.

"This is a case of stolen identity," Kuhn said. "It's a thing we all read about, but it never happens to us."

The impostor made the first three withdrawals, each for \$1,000, the same day as the address change on Jan. 14. The fourth withdrawal, for \$1,900, was made a day later.

In Jonesboro, Ga., the impostor showed up at a Western

Union office carrying a fake military identification card with Eugene Kuhn's name and Social Security number on it, Nancy Kuhn said credit union officials told her. The person knew Eugene's credit union savings account number and the date the account was opened. The only thing the impostor got wrong, Kuhn said, was her husband's birthdate.

Jack Simmonds, senior vice president of operations at Alaska USA, said the credit union asked Western Union to compare the signature at the wire service with the signature on the account. When they didn't match, the credit union reimbursed the Kuhns.

"I don't think people should be concerned," Simmonds said. "The credit union has made this person whole. The member has not lost any money."

Simmonds said the credit union's insurance company would probably investigate the fraud, along with the FBI.

He said that for security reasons he could not comment on account.
See THEFT, Page A-8

Fairbanks Daily News-Miner, Saturday, February 19, 2000

THEFT: Impostor steals \$4,900

Continued from Page A-1
cess accounts at the credit union. But he said credit union members have the option of having a password. "We take every reasonable step to keep accounts secure."

The credit union was almost too secure for Kuhn at one point. She said she closed one of the couple's accounts in a huff last fall because the credit union demanded both her driver's license number and her Social Security number for a withdrawal receipt. Kuhn said she was willing to show that information but re-

fused to let the bank put it on her receipt, in case it fell out of her purse or something, she said.

Kuhn said the credit union told her it would need the name, types of accounts at the credit union, Social Security number and date of birth from someone to access bank records. The couple is perplexed as to how someone could get that information, which is supposedly private.

Kuhn said her husband is "a little bit sloppy" but that he's never lost anything. "I don't think he ever misplaced one of

the statements. I keep track of those."

The couple opened the savings account in 1975, before the credit union was bought by Alaska USA, Kuhn said.

She and her husband don't know anybody in Jonesboro, which is a busy suburb of Atlanta.

Fairbanks police referred Kuhn's complaint to the FBI. Neither the Fairbanks FBI bureau or the Anchorage bureau have begun investigating.

Alaska State Legislature

Chairman,
Judiciary Committee
Administrative Regulations
Revenue Committee

Vice Chairman,
Resources Committee



Senator Robin L. Taylor

State Capitol
Juneau, Alaska 99801-1182
(907) 465-3873
Fax: (907) 465-3922

50 Front Street
Suite 203
Ketchikan, Alaska 99901
(907) 225-8088
Fax: (907) 225-0713

SB 259 Sponsor Statement Senate Bill

“An Act relating to criminal impersonation.”

Alaska has always been the “Last Frontier.” For most of us who came to this great state it was the mystique and adventure. For others it was a place to escape too. Unfortunately, some of the latter group are escaping from the law and have stolen someone else’s identity to do that.

Acting under an assumed name, with false identification to support the claim, they obtain credit cards and checking accounts often not paying the bills. This leaves honest Alaskans with the problem of dealing with Credit Agencies, or the government with little or no recourse.

But there is more than fraud to deal with. Criminal activities include, minors purchasing alcohol or tobacco or a person using someone’s good name to establish a less than acceptable reputation.

Once passed these additions to existing statute will give law enforcement an additional tool to keep Alaskans safer from fraud and deceit by those who with the use of false identification are not what they seem.

District A:

Hyder • Ketchikan • Kupreanof • Meyers Chuck • Petersburg • Saxman • Sitka • Wrangell

Alaska State Troopers



WHITE COLLAR CRIME SECTION

* * * * *

The White Collar Crime Section is charged with the duties of coordinating and or investigating selected acts of forgery, fraud, embezzlement, unsworn falsification, perjury, credit card crimes, politically sensitive matters, crimes which involve computers, to include forensic data recovery and analysis along with other investigations designated by the commander of the Criminal Investigation Bureau.

Currently, the White Collar Crime Section consists of one Sergeant and two Investigators. Investigators assigned to the White Collar Crime Section many times deal with complex cases that require many hours of document analysis in order to identify criminal violations. They work closely with prosecutors within the Department of Law's Office of Special Prosecutions and Appeals.

The Alaska State Trooper's White Collar Crime Section is a voting member of the National White Collar Crimes Center. This allows the section to draw on the many services and resources they provide, such as up to date training, data and document analysis, intelligence data bases, computer and network expertise and many other helpful tools that the white collar crime investigator may need.

Members of the White Collar Crime Section, while not auditors, have received specialized training in Fraud and Financial Crimes Investigative Techniques, Complex Crimes Case Management, the Investigation of Internet Crimes, and Computer Forensics.