

*DISCLAIMER: The following document is a **fictionalized indictment** used as the basis for a mock trial at the Black Hat 2007 conference. The events described did not occur. The characters are fictional and any resemblance to any person, living or dead is purely coincidental.*

Jury Instructions for Hacker Court 2007

Count 1: Fraud with counterfeit access device

In count one of the indictment, the government charges Mr. Nelson with violating 18 U.S.C. § 1029(a)(1). You may find Mr. Nelson guilty of this crime only if you are convinced that the government has proved each of the following beyond a reasonable doubt:

1. he produced, used, or trafficked in a counterfeit access device; and
2. he did so knowingly, and with the intent to defraud; and
3. his conduct affected interstate or foreign commerce.

Knowingly

You may conclude that Mr. Nelson acted “knowingly” only if the government proves beyond a reasonable doubt that he was aware of his act and did not act through ignorance, mistake, or accident. The government is not required to prove that he knew his act was unlawful. You may consider evidence of his words, acts, or omissions, along with all the other evidence, in deciding whether he acted knowingly.

Intent to defraud

You may conclude that Mr. Nelson acted “with the intent to defraud” only if the government proves beyond a reasonable doubt that he acted willfully with the intent to deceive or cheat. The essence of the crime is the willful use of a counterfeit access device with the intent to defraud, and the government does not need to prove that anyone was in fact deceived or defrauded.

Interstate or foreign commerce

The government does not need to prove that Mr. Nelson specifically intended to interfere with or affect interstate or foreign commerce. However, the government must prove that the natural consequence of his acts would be to affect interstate or foreign commerce.

For the purposes of count one, “interstate commerce” means the flow of commerce or business activities between two States. “Foreign commerce” means the flow of commerce or business activities between a State or the United States and a foreign country.

Access device

For the purposes of count one, a device is an “access device” only if each of the following is true:

1. the device is (a) a card, plate, code, account number, electronic serial number, mobile identification number, personal identification number; or (b) a telecommunications service, equipment, or instrument identifier; or (c) a means of account access; and
2. the device can be used alone, or together with another access device:
 - a. to obtain money, goods, services, or any other thing of value; or
 - b. to transfer funds, provided the transfer does not originate solely by a paper instrument.

Counterfeit access device

For the purposes of count one, a device is a “counterfeit access device” only if it is either:

1. an access device that is counterfeit, fictitious, altered or forged; or
2. an identifiable component of an access device or counterfeit access device.

Produces

For the purposes of count one, the term “produce” includes design, alter, authenticate, or assemble.

Traffics in

For the purposes of count one, the term “traffic” means transfer, or otherwise dispose of, to another, or to obtain control of with intent to transfer or dispose of.

Count 1 References

Generally

Criminal Pattern Jury Instruction Committee of the United States Court of Appeals for the Tenth Circuit, *Federal Jury Practice and Instructions, Criminal Pattern Jury Instructions: Tenth Circuit* 2.50.1 (2006).

Committee on Pattern Jury Instructions of the Judicial Council of the Eleventh Circuit, *Federal Jury Practice and Instructions, Pattern Jury Instructions: Eleventh Circuit, Criminal Cases with Annotations and Comments* 41.1 (2003).

Committee on Model Jury Instructions Ninth Circuit, *Federal Jury Practice and Instructions, Ninth Circuit Manual of Model Jury Instructions—Criminal Current through January 2007* 8.68 (2003).

Access device

18 U.S.C. § 1029(e)(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.)”).

U.S. v. Sepulveda, 115 F.3d 882 (11th Cir. 1997) (Unprogrammed ESN-MIN combinations constitute access devices within the meaning of §1029).

U.S. v. Dabbs, 134 F.3d 1071 (11th Cir. 1997)(A merchant account number constitutes an access device.)

Counterfeit access device

18 U.S.C. § 1029(e)(2).

U.S. v. Soape, 169 F.3d 257 at 262-64 (5th Cir. 1999) (counterfeit access devices include legitimate access devices procured by fraud.)

U.S. v. McCormick, 72 F.3d 1404 at 1408 (9th Cir. 1995) (submission of credit card application containing false or inflated information produces a counterfeit access device.)

U.S. v. Brannan, 898 F.2d 107 at 109 (9th Cir. 1990)(submitting fictitious credit card applications to bank was functional equivalent to manufacture of counterfeit access device.)

U.S. v. Luttrell, 889 F.2d 806 at 810 (9th Cir. 1989) (discusses distinction between unauthorized and counterfeit access devices), amended by 923 F.2d 764 (9th Cir. 1991)(en banc).

Intent to defraud

Pattern Crim. Jury Instr. 10th Cir. 2.50.1 (2006).

Pattern Crim. Jury Instr. 11th Cir. OI 41.1 (2003).

Model Crim. Jury Instr. 9th Cir. 3.17 (2003).

S.Rep.No. 368, 98th Cong., 2d Sess (“ [w]ith intent to defraud’ means that the offender has a conscious objective, desire or purpose to ‘deceive another person, and to induce such other person, in reliance upon such deception, to assume, create, transfer, alter, or terminate a right, obligation or power with reference to property.’)

H.R. Rep. No. 98-894, 98th Cong. 2d Sess. at 17 (1984) (“the term ‘with the intent’ in section 1029 should involve “the same culpable state of mind as the term ‘purpose’ as used in the Model Penal Code § 2.02.”).

Interstate commerce

Pattern Crim. Jury Instr. 10th Cir. 2.50.1 (2006).

Pattern Crim. Jury Instr. 11th Cir. OI 41.1 (2003).

U.S. v. Gomez, 87 F.3d 1093 at 1096-97 (9th Cir. 1996) (discussing role of the jury in determining a fact which is both an element of the offense and a jurisdictional fact.)

U.S. v. Lopez, 14 U.S. 549 (1995) (discusses the “affecting” commerce requirement.)

U.S. v. Clayton, 108 F.3d 1114 at 1117 (9th Cir. 1997) (applying the Lopez test to alleged violation of section 1029).

Knowingly

Model Crim. Jury Instr. 9th Cir. 5.6, 5.7 (2003).

Produces

18 U.S.C. § 1029(e)(4).

Traffics in

18 U.S.C. § 1029(e)(5).

Count 2: Use of protected computer for fraud

In count two of the indictment, the government charges Mr. Nelson with violating 18 U.S.C. § 1030(a)(4). You may find Mr. Nelson guilty of this crime only if you are convinced that the government has proved each of the following beyond a reasonable doubt:

1. he knowingly accessed a protected computer with the intent to defraud; and
2. his access either (a) was without authorization; or (b) was used to obtain information in the computer that he was not entitled to obtain; and
3. he used this access to further his fraud, and to obtain something of value; and
4. the object of his fraud, and the thing he obtained, either:
 - a. did not consist solely of use of the computer; or
 - b. consisted solely of use of the computer, and this use had value of more than \$5,000 in any one-year period.

Knowingly

You may conclude that Mr. Nelson acted “knowingly” only if the government proves beyond a reasonable doubt that he was aware of his act and did not act through ignorance, mistake, or accident. The government is not required to prove that he knew his act was unlawful. You may consider evidence of his words, acts, or omissions, along with all the other evidence, in deciding whether he acted knowingly.

Intent to defraud

You may conclude that Mr. Nelson acted “with the intent to defraud” only if the government proves beyond a reasonable doubt that he acted willfully with the intent to deceive or cheat.

Computer

For the purposes of count two, a device is a “computer” only if each of the following is true:

1. the device is an electronic, magnetic, optical, electrochemical, or high speed data processing device. A device may include any data storage or communication facilities directly related to or operating in conjunction with the device; and
2. the device is not an automated typewriter, typesetter, portable or hand-held calculator or other similar device; and
3. the device performs logical, arithmetic, or storage functions.

Protected computer

For the purposes of count two, a computer is a “protected computer” only if any one of the following is true:

1. the computer is exclusively for the use of a financial institution or the United States Government; or
2. the computer is used by or for a financial institution or the United States Government, and Mr. Nelson affected this use by accessing it; or
3. the computer is used in interstate commerce, or foreign commerce, or communication. This includes a computer located outside the United States that is used in a way that affects interstate commerce, foreign commerce, or communications in the United States.

Count 2 References

Generally

Committee on Model Jury Instructions Ninth Circuit, *Federal Jury Practice and Instructions, Ninth Circuit Manual of Model Jury Instructions—Criminal, Current through January 2007* 8.81 (2003).

Kevin F. O’Malley, Jay E. Grenig, Hon. William C. Lee, *Federal Jury Practice and Instructions, Criminal, Current through the 2007 Supplemental Service* 42.12 (5th ed.)

Computer

18 U.S.C. § 1030(e)(1) (“The term ‘computer’ means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and including 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 or hand held calculator, or other similar device.”)

Model Crim. Jury Instr. 9th Cir. 8.86A (2003).

Intent to defraud

S.Rep.No. 99 432 at 9 (1986) (“[A]” scheme ... to defraud should [not] fall under the ambit of § 1030(a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud. While such a tenuous link might be covered under current law where the instrumentality used is the mails or the wires, the Committee does not consider that link sufficient with respect to computers. To be prosecuted under this subsection the use of the computer must be more directly linked to the intended fraud. That is, it must be used by an offender ... to obtain property of another, which property furthers the intended fraud.”)

Model Crim. Jury Instr. 9th Cir. 3.17 (2003).

2A Fed. Jury. Prac. & Instr. 3.17 (5th ed.).

Knowingly

Model Crim. Jury Instr. 9th Cir. 5.6, 5.7 (2003).

2A Fed. Jury. Prac. & Instr. 8.77 Comment (5th ed.).

Protected computer

18 U.S.C. § 1030(e)(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, in-

cluding a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States.”)

Count 3: Damage to protected computer

In count three, the government charges Mr. Nelson with violating 18 U.S.C. § 1030(a)(5)(A)(i). You may find Mr. Nelson guilty of this crime only if you are convinced that the government has proved each of the following beyond a reasonable doubt:

1. he knowingly transmitted information, codes, programs, or commands; and
2. as a result of this transmission, he intentionally caused unauthorized damage to a protected computer; and
3. this damage resulted in loss to one or more persons in any one-year period, or loss resulting from a related course of conduct affecting one or more protected computers, aggregating at least \$5,000.

Knowingly

You may conclude that Mr. Nelson acted “knowingly” only if the government proves beyond a reasonable doubt that he was aware of his act and did not act through ignorance, mistake, or accident. The government is not required to prove that he knew his act was unlawful. You may consider evidence of his words, acts, or omissions, along with all the other evidence, in deciding whether he acted knowingly.

Computer

For the purposes of count three, a device is a “computer” only if each of the following is true:

1. the device is an electronic, magnetic, optical, electrochemical, or high speed data processing device. A device may include any data storage or communication facilities directly related to or operating in conjunction with the device; and
2. the device is not an automated typewriter, typesetter, portable or hand-held calculator or other similar device; and
3. the device performs logical, arithmetic, or storage functions.

Damage

For the purposes of count three, the term “damage” means any impairment to the integrity or availability of data, a program, a system, or information.

Loss

For the purposes of count three, the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

Person

For the purposes of count three, the term “person” means any individual, firm, corporation, educational institution, financial institution, government entity, or legal or other entity.

Protected computer

For the purposes of count three, a computer is a “protected computer” only if any one of the following is true:

1. the computer is exclusively for the use of a financial institution or the United States Government; or
2. the computer is used by or for a financial institution or the United States Government, and Mr. Nelson affected this use by transmitting information, codes, programs, or data to cause unauthorized damage to it; or
3. the computer is used in interstate commerce, or foreign commerce, or communication. This includes a computer located outside the United States that is used in a way that affects interstate commerce, foreign commerce, or communications in the United States.

Count 3 References

Generally

Committee on Pattern Jury Instructions of the Judicial Council of the Eleventh Circuit, *Federal Jury Practice and Instructions, Pattern Jury Instructions: Eleventh Circuit, Criminal Cases with Annotations and Comments* 42.3 (2003).

Committee on Model Jury Instructions Ninth Circuit, *Federal Jury Practice and Instructions, Ninth Circuit Manual of Model Jury Instruction—Criminal, Current through January 2007* 8.82 (2003).

Kevin F. O’Malley, Jay E. Grenig, Hon. William C. Lee, *Federal Jury Practice and Instructions, Criminal, Current through the 2007 Supplemental Service* 42.14 (5th ed.)

S. Rep. No. 104-357 at 11, 1996 WL 492169 at 25 (1996) (purpose of §1030(a)(5) is that persons authorized to access a computer face criminal liability only if they intend to cause damage.” Those not authorized are “punished for any intentional, reckless, or other damage they cause by their trespass.”)

Computer

18 U.S.C. § 1030(e)(1) (“The term ‘computer’ means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and including 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 or hand held calculator, or other similar device.”)

Damage

18 U.S.C. §1030(e)(8)

U.S. v. Middleton, 231 F.3d 1207 at 1211-12 (9th Cir. 2000) (discusses definitions of “protected computer” and “damage” prior to amendments to § 1030).

Knowingly

Model Crim. Jury Instr. 9th Cir. 5.6, 5.7 (2003).

2A Fed. Jury. Prac. & Instr. 8.77 Comment (5th ed.).

Loss

18 U.S.C. § 1030(e)(11).

9th Cir. Crim. Jury Instr. 8.86A (2003).

Person

18 U.S.C. § 1030(e)(12)

9th Cir. Crim. Jury Instr. 8.86A (2003).

Protected Computer

9th Cir. Crim. Jury Instr. 8.86A (2003).

18 U.S.C. § 1030(e)(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, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communications in the United States.”)

U.S. v. Middleton, 231 F.3d 1207 at 1211-12 (9th Cir. 2000) (discusses definitions of “protected computer” and “damage” prior to amendments to § 1030).