Primer

Computer Crimes

Prepared by the
Office of the General Counsel

DISCLAIMER

The Commission's legal staff publishes this document to assist in understanding and applying the sentencing guidelines. The information in this document should not be considered definitive or comprehensive. In addition, the information in this document does not necessarily represent the official position of the Commission on any particular issue or case, and it is not binding on the Commission, the courts, or the parties in any case. To the extent this document includes unpublished cases, practitioners should be cognizant of Fed. R. App. P. 32.1, as well as any corresponding rules in their jurisdictions.

Want to learn more about relevant statutes, case law, and guidelines on a specific topic? The Commission's legal staff offers a series of primers to assist in understanding and applying the sentencing guidelines on the following topics—

- Aggravating and Mitigating Role Adjustments
- Antitrust Offenses
- Categorical Approach
- Offenses Involving Commercial Sex Acts and Sexual Exploitation of Minors
- Computer Crimes
- Crime Victims' Rights
- Criminal History
- Departures and Variances
- Drug Offenses
- Economic Crime Victims
- Fines for Organizations
- Firearms Offenses
- Immigration Offenses
- Intellectual Property Offenses
- Loss Calculation under §2B1.1
- Relevant Conduct
- Retroactive Guideline Amendments
- RICO Offenses
- Selected Offenses Against the Person and VICAR
- Sexual Abuse and Failure to Register Offenses
- Supervised Release

Learn more at https://www.ussc.gov/guidelines/primers.

UNITED STATES SENTENCING COMMISSION
One Columbus Circle, N.E.
Suite 2-500, South Lobby
Washington, DC 20002-8002
T: (202) 502-4500
F: (202) 502-4699
www.ussc.gov ‖ @theusscgov

This document was produced and published at U.S. taxpayer expense.

TABLE OF CONTENTS

I. INTRODUCTION TO COMPUTER CRIMES

This primer provides a general overview of the federal statutes and guidelines for computer crimes. For purposes of this primer, "computer crimes" include offenses where the computer is the gravamen of the offense or sentencing enhancement.[1] As such, this primer primarily focuses on certain offenses found in 18 U.S.C. §§ 1030 and 1037, such as computer and email fraud, computer espionage, extortion relating to protected computers, and trespass on a government computer, and specific sentencing provisions within guidelines applicable to those offenses.[2] In addition, this primer discusses application of §3B1.3 (Abuse of Position of Trust or Use of Special Skill) in cases involving computers or the internet. Although the primer identifies some of the key cases and concepts, it is not a comprehensive compilation of authority nor intended to be a substitute for independent research and analysis of primary sources.

The primary statute for computer crimes is 18 U.S.C. § 1030 (Fraud and related activity in connection with computers), which prohibits computer fraud and abuse. Initially, section 1030 criminalized acts involving unauthorized access to a computer to obtain financial or government information, including national defense information, and the unauthorized access to computers operated for or on behalf of the United States government.[3] Over time, Congress amended the statute to include crimes such as trafficking in passwords and computer access, causing damage to a protected computer by transmission of a program, extortionate threats to damage a protected computer, and conspiracy to commit computer fraud.[4]

---

[1] Certain offenses may be committed using a computer, computer software, or the internet, but the use of the computer is incidental to the offense and not part of the statute or enhancement. These offenses are outside the scope of this primer. *See*, *e.g.*, United States v. Anwar, 741 F.3d 1134, 1135 (10th Cir. 2013) (making false threats to destroy building through email in violation of 18 U.S.C. § 844(e)); United States v. Humphreys, 352 F.3d 1175, 1176–77 (8th Cir. 2003) (making threats against the President of the United States through fax and in chat rooms in violation of 18 U.S.C. § 871(a)).

[2] Some of the statutes and guidelines referenced in this primer are explored in other primers prepared by the Commission. In those instances, this primer refers the reader to the primer that covers the topic in more specific detail. For example, the use of a computer in certain sex offenses is covered in detail in the Commission's primer on sexual abuse and failure to register offenses. *See* U.S. SENT'G COMM'N, PRIMER ON SEX OFFENSES: SEXUAL ABUSE AND FAILURE TO REGISTER OFFENSES (2021), https://www.ussc.gov/guidelines/primers/sexual-abuse-and-failure-register-offenses.

[3] Congress enacted the computer fraud statute at section 1030 as part of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Pub. L. No. 98–473, § 2102(a), 98 Stat. 2190.

[4] *See*, *e.g.*, Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, § 2, 100 Stat. 1213 (trafficking in passwords and computer access); Computer Abuse Amendments Act of 1994, Pub. L. No. 103–322, § 290001(b), 108 Stat. 2097, 2098 (unlawful transmission of a program, information, code, or command); National Information Infrastructure Protection Act of 1996, Pub. L. No. 104–294, § 201, 110 Stat. 3491, 3492 (extortionate threats to damage protected computer); Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110–326, § 206, 122 Stat. 3561, 3563 (conspiracy to commit computer fraud). Congress continues to consider legislation on computer fraud and abuse given technological advances. *See generally* PETER G. BERRIS, CONG. RSCH. SERV., R46536, CYBERCRIME AND THE LAW: COMPUTER FRAUD AND ABUSE ACT (CFAA) AND THE 116TH CONGRESS (2020).

Section 1030(a) currently prohibits:

(1) *Computer espionage*.—Knowing access to a computer without authorization (or exceeding authorized access), obtaining protected information, and willful communication or retention of such information with reason to believe it could be used to the injury of the United States or the advantage of a foreign nation;[5]

(2) *Unauthorized access to information*.—Intentional and unauthorized access (or exceeding authorized access) to a computer and obtaining information (A) contained in a financial record or in a file of a consumer reporting agency, (B) from a United States department or agency, or (C) from any protected computer;[6]

(3) *Trespassing on a government computer*.—Intentional and unauthorized access to a nonpublic government computer, or to a computer used by or for the United States government that affects such use;[7]

(4) *Computer fraud*.—Unauthorized access (or exceeding authorized access) to a protected computer, with the intent to defraud, in furtherance of that fraud, and where something of value is obtained;[8]

(5) *Intentional damage or loss by transmission of program or unauthorized access*.—Knowing transmission of a program, information, code, or command resulting in intentional damage to a protected computer, or intentional unauthorized access to a protected computer resulting in damage or loss;[9]

(6) *Trafficking in passwords and computer access information*.—Knowingly and with intent to defraud trafficking in passwords or similar computer access information if the computer is used by or for the United States government or such trafficking affects interstate commerce;[10] and

---

[5] 18 U.S.C. § 1030(a)(1). Computer espionage is a "Federal crime of terrorism," as defined in 18 U.S.C. § 2332b, if the offense "is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct." 18 U.S.C. § 2332b(g)(5). Computer espionage under section 1030(a)(1) and its related guideline (§2M3.2) are discussed in detail below. *See infra* Part II.

[6] 18 U.S.C. § 1030(a)(2). Offenses relating to computer fraud, such as those found in subsections (a)(2) and (a)(4)–(6), and the related guideline (§2B1.1) are discussed in detail below. *See infra* Part III.

[7] *Id.* § 1030(a)(3). Computer trespass under section 1030(a)(3) and its related guideline (§2B2.3) is discussed in detail below. *See infra* Part IV.

[8] *Id.* § 1030(a)(4).

[9] *Id*. § 1030(a)(5). A violation of section (a)(5)(A) that results in damage as defined in section 1030(c)(4)(A)(i)(II)–(VI) is a "Federal crime of terrorism," as defined in 18 U.S.C. § 2332b, if the offense "is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct." 18 U.S.C. § 2332b(g)(5).

[10] 18 U.S.C. § 1030(a)(6).

> (7) *Extortion involving protected computers*.—Transmitting a threatening communication or demand relating to protected computers with the intent to extort from any person any money or thing of value.[11]

Through section 1030(b), the statute further prohibits attempt and conspiracy to commit the above offenses.[12]

Section 1030(e)(1) defines a "computer" as an "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions[.]"[13] As such, cell phones and devices with data processors are "computers" within the meaning of the statute.[14] A "protected computer" is 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;
>
> (B) which is used in or affecting 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 communication of the United States; or
>
> (C) that—
>
> (i) is part of a voting system; and
>
> (ii)
>
> (I) is used for the management, support, or administration of a Federal election; or
>
> (II) has moved in or otherwise affects interstate or foreign commerce.[15]

The statute defines "loss" as "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,

---

[11] *Id.* § 1030(a)(7). Extortion relating to protected computers under section 1030(a)(7) and its related guideline (§2B3.2) is discussed in detail below. *See infra* Part V.

[12] *Id.* § 1030(b).

[13] *Id.* § 1030(e)(1). The definition expressly excludes automated typewriters, typesetters, portable hand-held calculators, and similar devices. *Id.*

[14] *See, e.g.*, United States v. Mathis, 767 F.3d 1264, 1283 (11th Cir. 2014) (cell phone qualifies as "computer" under § 1030(e)), *overruled on other grounds as stated in* United States v. Johnson, 681 F. App'x 735 (11th Cir. 2017); United States v. Kramer, 631 F.3d 900, 902–04 (8th Cir. 2011) (same); *see also* United States v. Mitra, 405 F.3d 492, 495 (7th Cir. 2005) ("As more devices come to have built-in intelligence, the effective scope of the statute grows.").

[15] 18 U.S.C. § 1030(e)(2).

cost incurred, or other consequential damages incurred because of interruption of service."[16] It defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[17]

In addition to other terms, the statute defines "exceeds authorized access" as "access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[18] The statute does not define the terms "authorization" or "without authorization," and courts have interpreted those terms and the phrase "exceeds authorized access" in different ways.[19]

Section 1030(c) establishes the penalties for an offense under this statute. Criminal punishment for a violation of section 1030 ranges from misdemeanor punishment up to life in prison, depending on the offense of conviction.[20] The statute provides for increased punishment for certain offenses if the offense was committed under aggravating circumstances and for subsequent violations of section 1030.[21]

The following sections discuss computer crimes described in sections 1030 and 1037 and the applicable guidelines provisions in more detail.

---

16 *Id.* § 1030(e)(11).

17 *Id.* § 1030(e)(8).

18 *Id.* § 1030(e)(6).

19 *See* CHARLES DOYLE, CONG. RSCH. SERV., 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 15–16 (2014) ("[T]he courts have experienced some difficulty applying the terms 'without authorization' and 'exceeds authorized access' as used in paragraph 1030(a)(2) and the other paragraphs of 18 U.S.C. 1030 . . . ."). *Compare* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (" '[E]xceeds authorized access' in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*."), *with* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) ("[The defendant] exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason."), *and* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) ("The question before us is whether 'authorized access' or 'authorization' may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system. We conclude that it may, at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime."). The Supreme Court granted certiorari to address the issue, which may resolve the differences in approach. United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 140 S. Ct. 2667 (2020) (No. 19–783). *See also* Brief for Petitioner at (i), *Van Buren*, 140 S. Ct. 2667 (2020) (No. 19–783) ("Question Presented: Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.").

20 18 U.S.C. § 1030(c). Penalty provisions for specific subsections in § 1030 are discussed in more detail below.

21 *See id.* The statute also provides for civil actions to obtain compensatory damages and injunctive relief or other equitable relief. *See id.* § 1030(g).

II. COMPUTER ESPIONAGE

A. RELEVANT STATUTE: 18 U.S.C. § 1030(A)(1) (COMPUTER ESPIONAGE)

Section 1030(a)(1) prohibits "computer espionage," that is, the willful communication to any unauthorized person, or willful retention, of protected information or restricted data, obtained by knowingly accessing a computer without authorization (or exceeding authorized access), with reason to believe that such information or data could be used to the injury of the United States or to the advantage of a foreign nation.[22] A defendant faces up to ten years of imprisonment for a violation of section 1030(a)(1) unless the defendant has a prior conviction for a section 1030 offense, in which case the statutory maximum punishment is 20 years.[23]

B. APPLICABLE GUIDELINE: SECTION 2M3.2 (GATHERING NATIONAL DEFENSE INFORMATION)

The applicable guideline for offenses under section 1030(a)(1) is §2M3.2.[24] Section 2M3.2 includes two alternate base offense levels: 35, if top secret information was gathered, or 30 otherwise.[25] The offense levels are based on the classification of the information involved in the offense, which reflects the importance of the information to the national security and reflects the potential harm or loss resulting from gathering or transmission of national defense information.[26] Section 2M3.2 does not have any specific offense characteristics.

The Commentary to §2M3.2 incorporates by reference the Commentary to §2M3.1 (Gathering or Transmitting National Defense Information to Aid a Foreign Government),

---

22 18 U.S.C. § 1030(a)(1).

23 *Id.* § 1030(c)(1). As stated above, the 18 U.S.C. § 1030 statute also provides for civil actions and penalties. See 18 U.S.C. § 1030(g), and violations of section 1030(a)(1) calculated "to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct" constitute a "Federal crime of terrorism" as defined in 18 U.S.C. § 2332b. *See* 18 U.S.C. §§ 1030(g) and 2332b(g)(5)(B)(i).

24 U.S. SENT'G COMM'N, *Guidelines Manual*, App. A. (Nov. 2018) [hereinafter USSG].

25 USSG §2M3.2(a). The Ninth Circuit has held that "the offense level distinctions do not require that the information gathered be classified" for purposes of §2M3.2, because the offense levels only refer to "top secret information" or "otherwise." United States v. Chung, 659 F.3d 815, 834–35 (9th Cir. 2011).

26 USSG §2M3.1, comment. (backg'd) ("Offense level distinctions in this subpart are generally based on the classification of the information gathered or transmitted. This classification, in turn, reflects the importance of the information to the national security."); USSG §2M3.1, comment. (n.2) ("The Commission has set the base offense level in this subpart on the assumption that the information at issue bears a significant relation to the nation's security, and that the revelation will significantly and adversely affect security interests."); *see also* U.S. SENT'G COMM'N, 2003 REPORT TO THE CONGRESS: INCREASED PENALTIES FOR CYBER SECURITY OFFENSES 7 (2003) [hereinafter 2003 REPORT TO CONGRESS ON CYBER SECURITY OFFENSES], https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/computer-crime/200304_RtC_Increased_Penalties_Cyber_Security.pdf ("The potential harm, including loss, involved in violations of 18 U.S.C. § 1030(a)(1) . . . which are referenced to §2M3.2 . . . is accounted for by the high base offense levels in that guideline.").

including its definitions and departure considerations.[27] "Top secret information" is defined as information that, if disclosed, "reasonably could be expected to cause exceptionally grave damage to the national security."[28] Pursuant to the Commentary to §2M3.1, a downward departure may be warranted if revelation of the defense information is likely to cause little or no harm.[29] The Commentary also provides that the court may depart from the guidelines if the President or the President's designee represents that imposition of a sanction other than one authorized by the guidelines is necessary to protect national security or further the nation's foreign policy objectives.[30]

III. COMPUTER FRAUD

A. RELEVANT STATUTES

1. 18 U.S.C. § 1030(a)(2) and (a)(4)–(6) (Computer Fraud and Access)

As stated above, sections 1030(a)(2) and (a)(4)–(6) prohibit unauthorized access to a computer and obtaining information, computer fraud, intentional damage or loss without

[27] USSG §2M3.2, comment. (n.1).

[28] USSG §2M3.1, comment. (n.1). The definition of "top secret information" is derived from an Executive Order. *See id.; see also* Exec. Order No. 13526, 75 FR 707 (Dec. 29, 2009) (" 'Top Secret' shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe."); USSG App. C, amends. 746 (effective Nov. 1, 2010) and 778 (effective Nov. 1, 2013) (updating references to ensure Executive Order to which it refers is the most recent Executive Order).

[29] USSG §2M3.1, comment. (n.2).

[30] USSG §2M3.1, comment. (n.3). The other application note in §2M3.2 instructs that, for convictions under 18 U.S.C. § 793(d) or (e), the guideline at §2M3.3 (Transmitting National Defense Information; Disclosure of Classified Cryptographic Information; Unauthorized Disclosure to a Foreign Government or a Communist Organization of Classified Information by Government Employee; Unauthorized Receipt of Classified Information) may apply. USSG §2M3.2, comment. (n.2). In turn, Application Note 2 to §2M3.3 provides that if the defendant is convicted of § 793(d) or (e) for the willful transmission or communication of intangible information with reason to believe it could be used to the injury of the United States or the advantage of a foreign nation, the court applies §2M3.2. USSG §2M3.3, comment. (n.2). The court must consider the offense conduct charged in the defendant's count of conviction to determine whether §2M3.2 or §2M3.3 is the appropriate guideline for the case under consideration. *See* USSG §1B1.2, comment. (n.1) ("In the case of a particular statute that proscribes a variety of conduct that might constitute the subject of different offense guidelines, the Statutory Index may specify more than one offense guideline for that particular statute, and the court will determine which of the referenced guideline sections is most appropriate for the offense conduct charged in the count of which the defendant was convicted."); *see also* United States v. Malki, 609 F.3d 503, 510 (2d Cir. 2010) ("Since the conduct of 'retain[ing],' which Makli acknowledged in his guilty plea, is similar to 'unauthorized receipt' and significantly different from 'gathering,' it seems clear that section 2M3.3, rather than section 2M3.2, is the appropriate guideline for his case."); United States v. Aquino, 555 F.3d 124, 131 (3d Cir. 2009) (vacating and remanding for resentencing when court applied §2M3.2 rather than §2M3.3 because the "offense is unambiguously excluded from punishment under § 2M3.2 by virtue of both the format of the national defense information in his possession (tangible) and the conduct to which he pleaded (retention).").

authorization by transmission of a program or code, and trafficking in passwords or similar computer access information, respectively.

Section 1030(a)(2) relates to offenses that involve obtaining information by hacking a computer or exceeding authorized access to a computer.[31] Violations of section (a)(2) are punishable by not more than one year in prison unless (1) the offense was committed for purposes of commercial advantage or private financial gain or in furtherance of a criminal or tortious act, or the value of the information exceeds $5,000, in which case the defendant faces up to five years' imprisonment, or (2) the defendant has a prior conviction for an offense under section 1030, in which case the maximum prison term is ten years.[32]

Section (a)(4) prohibits unauthorized access, or exceeding authorized access, to a protected computer with the intent to defraud, in furtherance of that fraud, and where something of value is obtained.[33] Violations of section (a)(4) are punishable by not more than five years in prison unless the defendant has a prior conviction for an offense under section 1030, in which case the statutory maximum is ten years of imprisonment.[34]

Section 1030(a)(5) prohibits knowingly causing the transmission of a program or code and intentionally causing damage to a protected computer.[35] Penalties for a violation

---

[31] *See*, *e.g.*, United States v. Gasperini, 894 F.3d 482, 485–86 (2d Cir. 2018) (computer hacking, gaining access to information on computers, taking usernames and passwords); United States v. John, 597 F.3d 263, 269 (5th Cir. 2010) (Citigroup account manager accessed and printed customer information and provided it to co-conspirators to incur fraudulent changes on customers' accounts). As stated above, courts have interpreted those terms and the phrase "exceeds authorized access" in different ways, and the Supreme Court granted certiorari to address the issue. *See supra* note 19 and accompanying text.

[32] 18 U.S.C. § 1030(c)(2).

[33] *Id.* § 1030(a)(4); *see*, *e.g.*, United States v. Gasperini, No. 16-CR-441, 2017 WL 2399693, at *3–6 (E.D.N.Y. June 1, 2017) (denying motion to dismiss indictment in "click fraud" scheme against advertising companies). *But see* United States v. Nosal, 676 F.3d 854, 864 (9th Cir. 2012) (affirming dismissal of counts "[b]ecause Nosal's accomplices had permission to access the company database and obtain the information contained within, the government's charges fail to meet the element of 'without authorization, or exceeds authorized access' under 18 U.S.C. § 1030(a)(4)"); United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997) (reversing conviction; "Czubinski unquestionably exceeded authorized access to a Federal interest computer . . . . [However, we] find[] that his searches of taxpayer return information did not satisfy the statutory requirement that he obtain 'anything of value.' . . . The government failed, however, to prove that Czubinski intended anything more than to satisfy idle curiosity.").

[34] 18 U.S.C. § 1030(c)(3).

[35] *Id.* § 1030(a)(5); *see*, *e.g.*, United States v. Gammell, 932 F.3d 1175 (8th Cir. 2019) (upholding armed career criminal status and restitution order in case involving conspiracy to cause intentional damage to a protected computer where defendant used distributed denial of service ("DDoS") attacks against companies, law enforcement agencies, and court systems). As stated above, a violation of section (a)(5)(A) that results in damage as defined in 1030(c)(4)(A)(i)(II)–(VI) is a "Federal crime of terrorism," as defined in 18 U.S.C. § 2332b, if the offense "is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct." 18 U.S.C. § 2332b(g)(5). Damage as described in subsections 1030(c)(4)(A)(i)(II)–(VI) includes impairment of the medical treatment or care of an individual, physical injury to another, and threats to public safety, among others. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(II)–(VI).

of section (a)(5) range from one year to life imprisonment.[36] For example, a defendant faces up to five years of imprisonment if the offense caused damage affecting ten or more protected computers during any one-year period.[37] If a defendant attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A) (knowing transmission of a code or similar information that intentionally causes damage to protected computer), the defendant faces up to life in prison.[38]

Section 1030(a)(6) prohibits knowingly, and with intent to defraud, trafficking in passwords or similar access information.[39] Violations of section (a)(6) are punishable by not more than one year in prison unless the defendant has a prior conviction for an offense under section 1030, in which case the statutory maximum is ten years of imprisonment.[40]

2. 18 U.S.C. § 1037 (Fraud and Related Activity in Connection with Electronic Mail)

Section 1037 prohibits certain activities relating to the transmission of multiple commercial email messages. The statute prohibits the transmission of multiple emails in conjunction with the following acts: (1) unauthorized access to a protected computer; (2) use of a protected computer with the intent to mislead recipients or any internet access service as to the messages' origin; (3) material falsification of header information in multiple commercial email messages; (4) registration by material falsification of identity for five or more email accounts (or online user accounts) or two or more domain names; or (5) false representation as a registrant of five or more Internet Protocol (IP) addresses.[41] The statute defines "multiple" as "more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period."[42] Punishment for an offense under section 1037 depends on the offense of conviction and whether specific aggravating factors exist, and ranges from misdemeanor punishment to a 3- or 5-year statutory maximum term of imprisonment.[43]

---

[36] 18 U.S.C. § 1030(c)(4).

[37] *Id.* § 1030(c)(4)(A)(i)(VI).

[38] *Id.* § 1030(c)(4)(F).

[39] *Id.* § 1030(a)(6).

[40] *Id.* § 1030(c)(2)(A) and (c)(2)(C).

[41] *Id.* § 1037(a)(1)–(5).

[42] *Id.* § 1037(d)(3). The statute also provides definitions or references other statutory definitions for terms such as "loss" and "materially." *Id.* § 1037(d)(1)–(2).

[43] *See id.* § 1037(b). For example, a violation of section 1037 is set at a maximum term of five years' imprisonment if the offense was committed in furtherance of a felony or the defendant has a prior conviction under §§ 1037, 1030, or a state statute that involves similar conduct. *Id.* § 1037(b)(1). A maximum penalty of three years of imprisonment is set for offenses: (1) under subsection (a)(1), (2) under subsection (a)(4) that involve 20 or more falsified email account or domain name registrations, (3) that involve email messages exceeding threshold amounts (*e.g.*, 2,500 in a 24-hour period), (4) that caused loss aggregating $5,000 or

B. Applicable Guideline: Section 2B1.1 (Theft, Property Destruction, and Fraud)

Violations of 18 U.S.C. §§ 1030(a)(2), (a)(4), (a)(5), and (a)(6) and 1037 are referenced in Appendix A (Statutory Index) of the *Guidelines Manual* to §2B1.1, the guideline for theft, property destruction, and fraud offenses.[44]

1. Base Offense Levels

Section 2B1.1(a) includes two alternative base offense levels (BOL). The higher of the two, BOL 7, applies when the defendant was convicted of an offense "referenced to this guideline" and "that offense of conviction has a statutory maximum term of imprisonment of 20 years or more."[45] If these conditions are not met, then the lower BOL of 6 applies.

The Commentary to the guideline explains that the term "referenced to this guideline" means that Appendix A either directly references the offense of conviction to §2B1.1,[46] or, in the case of a conviction for conspiracy, solicitation, or attempt, §2B1.1 is the appropriate guideline for the offense the defendant was conspiring, soliciting, or attempting to commit.[47] "Statutory maximum term of imprisonment," for purposes of this guideline, means the maximum term of imprisonment authorized for the offense of conviction, including any increase under a statutory enhancement.[48]

---

more in value over one year, (5) where a defendant obtained anything of value aggregating $5,000 or more over one year, or (6) where the defendant was an organizer or leader over three or more persons. *Id.* § 1037(b)(2). Otherwise, the maximum penalty for an offense under section 1037 is not more than one year in prison. *Id.* § 1037(b)(3).

[44] *See* USSG App. A. Computer crimes may also involve mail, wire, and bank fraud or involve trade secrets or intellectual property. Section 2B1.1, which is discussed in detail in this section, is the applicable guideline for defendants convicted under the mail, wire, and bank fraud statutes (except those offenses more appropriately sentenced under §2C1.1 (Bribery)). *Id.* The applicable guideline for crimes involving criminal infringement of copyright or trademark is §2B5.3 (Criminal Infringement of Copyright or Trademark). For more information regarding the sentencing of intellectual property crimes, see U.S. Sent'g Comm'n, Primer on Intellectual Property (2021), https://www.ussc.gov/guidelines/primers/intellectual-property.

[45] USSG §2B1.1(a)(1).

[46] USSG §2B1.1, comment. (n.2(A)). For purposes of this BOL, §2B1.1 must be the applicable Chapter Two guideline specifically referenced in Appendix A for the offense of conviction, as determined by §1B1.2 (Applicable Guidelines). *Id.*; *see also* USSG §1B1.2(a) ("Determine the offense guideline section in Chapter Two (Offense Conduct) applicable to the offense of conviction (*i.e.*, the offense conduct charged in the count of the indictment or information of which the defendant was convicted).").

[47] USSG §2B1.1, comment. (n.2(A)). Specifically, if the defendant has a conviction for conspiracy, solicitation, or attempt and §2X1.1 (Attempt, Solicitation, or Conspiracy) applies, the offense is "referenced to this guideline" if §2B1.1 is the appropriate guideline for the offense the defendant was convicted of conspiring, soliciting, or attempting to commit. *Id.*; *see also* §1B1.2(a) ("If the offense involved a conspiracy, attempt, or solicitation, refer to §2X1.1 (Attempt, Solicitation, or Conspiracy) as well as the guideline referenced in the Statutory Index for the substantive offense.").

[48] USSG §2B1.1, comment. (n.2(B)).

While many offenses involving computer fraud sentenced under §2B1.1 will likely start with a BOL of 6, some offenses may start with the alternative BOL of 7 because the defendant was convicted of an offense referenced to §2B1.1 that has a 20-year statutory maximum penalty. For example, a defendant convicted of an offense under 18 U.S.C. § 1030(a)(5)(A) (knowing transmission of a code or similar information that intentionally causes damage to a protected computer), where the defendant attempts to cause or knowingly or recklessly causes serious bodily injury, starts with a BOL of 7, because section 1030(c)(4)(E) (the relevant punishment provision) calls for a term of imprisonment of "not more than 20 years."[49] In contrast, a defendant convicted of unauthorized access to information under section 1030(a)(2), where the offense was committed for purposes of commercial advantage or financial gain, starts with a BOL of 6 because its statutory maximum penalty is five years of imprisonment.[50]

2. Specific Offense Characteristics

Section 2B1.1 has 20 specific offense characteristics (SOCs), some of which relate to conduct that occurs in computer crimes specifically. This section covers the SOCs in §2B1.1 that commonly apply to computer fraud cases and that capture certain aggravating factors that are often present in computer crimes.

a. Loss

Section 2B1.1(b)(1) raises offense levels incrementally based on the amount of loss involved in the offense. Loss is a measure of the pecuniary or monetary harm resulting from the offense or that the defendant intended to cause. The amount of loss is a driving factor in determining the offense level in most fraud cases, including computer fraud offenses.[51] The government must prove loss by a preponderance of the evidence.[52] The court need only make a reasonable estimate of the loss and is entitled to appropriate deference in its determination.[53]

The Commentary to §2B1.1 provides instructions to the court regarding loss amount determinations, including how to calculate loss, what constitutes loss, and what factors to consider in determining loss, and provides special rules for determining loss in

[49] *See* 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(E).

[50] *See id.* § 1030(a)(2) and (c)(2)(B).

[51] *See* USSG §2B1.1, comment. (backg'd) ("[A]long with other relevant factors under the guidelines, loss serves as a measure of the seriousness of the offense and the defendant's relative culpability and is a principal factor in determining the offense level under this guideline.").

[52] *See, e.g.*, United States v. Lacerda, 958 F.3d 196, 214 (3d Cir. 2020); United States v. Flete-Garcia, 925 F.3d 17, 28 (1st Cir. 2019); United States v. Pu, 814 F.3d 818, 825 (7th Cir. 2016).

[53] USSG §2B1.1, comment. (n.3(C)); *see also* 18 U.S.C. § 3742(e) and (f).

certain types of cases.[54] The guideline instructs that loss is the greater of the actual or intended loss.[55] "Actual loss" is the reasonably foreseeable pecuniary harm resulting from the offense.[56] "Intended loss" is the pecuniary harm the defendant purposely sought to inflict and includes intended pecuniary harm that would be impossible or unlikely to occur.[57] The guideline provides a non-exhaustive list of factors for the court to consider in its loss estimation:

(i) The fair market value of the property unlawfully taken, copied, or destroyed; or, if the fair market value is impracticable to determine or inadequately measures the harm, the cost to the victim of replacing that property;

(ii) In the case of proprietary information (*e.g.*, trade secrets), the cost of developing that information or the reduction in the value of that information that resulted from the offense;

(iii) The cost of repairs to damaged property;

(iv) The approximate number of victims multiplied by the average loss to each victim;

(v) The reduction that resulted from the offense in the value of equity securities or other corporate assets; and

(vi) More general factors, such as the scope and duration of the offense and revenues generated by similar operations.[58]

"Loss" does not include costs such as interest, penalties, or finance charges, nor does it include costs to the government in its criminal investigation or prosecution of an offense.[59]

---

[54] *See* USSG §2B1.1, comment. (n.3). For a guide to determining loss under §2B1.1(b)(1) generally, see U.S. SENT'G COMM'N, PRIMER ON LOSS CALCULATIONS UNDER §2B1.1(B)(1) (2021), https://www.ussc.gov/guidelines/primers/loss-calculation [hereinafter LOSS CALCULATIONS PRIMER].

[55] USSG §2B1.1, comment. (n.3(A)); *see also* United States v. Ayelotan, 917 F.3d 394, 408 (5th Cir.) (stating, in a case involving cybercrimes, "[t]he Sentencing Guidelines don't require the defendant to have intended the *specific* loss amount. Instead, the district court simply has to conclude that the defendant knew or reasonably should have known that the scheme would cause the harm."), *cert. denied*, 140 S. Ct. 123 (2019).

[56] USSG §2B1.1, comment. (n.3(A)(i)). For purposes of §2B1.1, "pecuniary harm" means monetary harm or harm otherwise readily measurable in money, while "reasonably foreseeable pecuniary harm" means pecuniary harm that the defendant knew or reasonably should have known was a potential result of the offense. USSG §2B1.1, comment. (n.3(A)(iii)–(iv)).

[57] USSG §2B1.1, comment. (n.3(A)(ii)).

[58] USSG §2B1.1, comment (n.3(C)). In 2009, the Commission amended Application Note 3(C)(i) to, among other things, address cases where the owner retains possession of the information, but the value of the information is reduced once copied. *See* USSG App. C, amend. 726 (effective Nov. 1, 2009) ("The amendment recognizes, for example, that a computer crime that does not deprive the owner of the information in the computer nonetheless may cause loss inasmuch as it reduces the value of the information. The amendment makes clear that in such a case the court may use the fair market value of the copied property to estimate loss.").

[59] USSG §2B1.1, comment. (n.3(D)).

The Commentary to §2B1.1 includes specific rules for determining loss in computer fraud cases under section 1030, which apply in addition to the general rules discussed above. First, for section 1030 offenses, actual loss includes any reasonable cost to any victim regardless of whether such harm was reasonably foreseeable.[60] Under this rule, "any reasonable cost to any victim" includes the cost of responding to the offense; damage assessments; restoration of data, programs, systems, or information; and any lost revenue or other damages incurred because of interruption of service.[61] Courts have interpreted loss in this context to include costs such as lost productivity, the cost of switching internet providers,[62] and the difference in the cost of in-state tuition and out-of-state tuition along with lost revenue and the cost of retaking classes.[63]

Second, in cases involving stolen or counterfeit credit cards and unauthorized access devices, loss includes unauthorized charges made with the device. The guidelines also set a minimum loss amount for each of these items as not less than either $500 per access device, or $100 if the device is a means of telecommunications access that identifies a specific account or telecommunications instrument that was only possessed and not used.[64]

b. Mass marketing

Section 2B1.1(b)(2) provides a graduated increase if certain circumstances exist, which includes a 2-level increase for mass-marketing that could apply to cases involving computer fraud.[65] The Commentary to §2B1.1 defines "mass-marketing" as a "plan,

[60] USSG §2B1.1, comment. (n.3(A)(v)(III)). This distinguishes loss involving computer fraud from the general definition of "actual loss," which, as discussed above, requires reasonable foreseeability of pecuniary harm.

[61] *Id.* This rule parallels the definition of "loss" in section 1030. *See* 18 U.S.C. § 1030(e)(11).

[62] For instance, in a case involving access and damage to a protected computer by a former employee, the Seventh Circuit upheld the district court's consideration of lost productivity and the cost of switching internet providers. United States v. Schuster, 467 F.3d 614, 617 (7th Cir. 2006). The court further stated that it could not conclude that costs incurred by victims in responding to defense subpoenas and testifying were "costs primarily [incurred] to aid the government" in prosecution or investigation of an offense, but even if it presumed so, the district court's inclusion of those losses in its calculation was harmless. *Id.* at 620.

[63] For example, in a case involving alteration of grades and students' status as in-state residents at Florida A&M University, the Eleventh Circuit upheld a finding that loss included the difference in the cost of in-state tuition and out-of-state tuition, along with lost revenue and the cost of retaking classes. United States v. Barrington, 648 F.3d 1178, 1197–98 (11th Cir. 2011).

[64] USSG §2B1.1, comment (n.3(F)(i)). This provision states: "In a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than $500 per access device. However, if the unauthorized access device is a means of telecommunications access that identifies a specific telecommunications instrument or telecommunications account (including an electronic serial number/mobile identification number (ESN/MIN) pair), and that means was only possessed, and not used, during the commission of the offense, loss shall be not less than $100 per unused means." *Id.*

[65] Section 2B1.1 provides the following graduated increase in subsection (b)(2):

program, promotion, or campaign that is conducted through solicitation by telephone, mail, the Internet, or other means to induce a large number of persons to (i) purchase goods or services; (ii) participate in a contest or sweepstakes; or (iii) invest for financial profit."[66] The Commentary also instructs that this 2-level enhancement should be applied to any defendant convicted of section 1037 (Fraud and related activity in connection with electronic mail) offenses or who committed an offense involving conduct described in section 1037, unless the defendant meets the criteria for a greater enhancement provided for in §2B1.1(b)(2).[67]

Use of the internet to solicit and induce a large number of persons to purchase goods, participate in a contest, or invest for financial profit through online advertisements or specific websites dedicated to the furtherance of the scheme can be sufficient to trigger the mass-marketing enhancement.[68]

(Apply the greatest) If the offense—

(A) (i) involved ten or more victims; (ii) was committed through mass-marketing; or (iii) resulted in substantial financial hardship to one or more victims, increase by **2** levels;

(B) resulted in substantial financial hardship to five or more victims, increase by **4** levels; or

(C) resulted in substantial financial hardship to 25 or more victims, increase by **6** levels.

USSG §2B1.1(b)(2). For a general overview of guideline issues related to victims in offenses sentenced under §2B1.1, see U.S. SENT'G COMM'N, PRIMER ON ECONOMIC CRIME VICTIMS (2021), https://www.ussc.gov/guidelines/primers/economic-crime-victims.

[66] USSG §2B1.1, comment. (n.4(A)); *see also* 18 U.S.C. § 2325 (defining the term "telemarketing or email marketing").

[67] USSG §2B1.1, comment. (n.4(B)); *see also* USSG App. C, amend. 665 (effective Nov. 1, 2004) (where the Reason for Amendment states that "[b]ecause each offense under 18 U.S.C. § 1037 contains as an element the transmission of multiple commercial electronic messages . . . the amendment provides in Application Note 4 that the mass-marketing enhancement in §2B1.1(b)(2)(A)(ii) shall apply automatically to any defendant who is convicted of 18 U.S.C. § 1037, or who committed an offense involving conduct described in 18 U.S.C. § 1037.").

[68] *See* United States v. Feldman, 647 F.3d 450, 461 (2d Cir. 2011) (enhancement upheld where defendant registered and used a website named "liver4you.org" in a scheme to defraud individuals seeking organ transplants: "[A] single public website on the internet can, and is designed to, reach a large number of people, [and] use of such a website to induce people to enter a fraud can vastly increase the scale of the fraud . . . ."); United States v. Christiansen 594 F.3d 571, 576 (7th Cir. 2010) (enhancement upheld where defendant posed as expectant mother seeking adoption of "child" then responded to inquiries online: "the fact that Christiansen posted an online advertisement that was open to the public shows that she designed her scheme to induce a large number of victims."); United States v. Hall, 604 F.3d 539, 545–46 (8th Cir. 2010) (while "mere use of a website is not sufficient to trigger" the enhancement, "[t]he mere fact Hall operated a website devoted to the solicitation of investments in his fraudulent scheme is sufficient."); United States v. Kieffer, 621 F.3d 825, 834–35 (8th Cir. 2010) (district court did not err in applying the enhancement where defendant, posing as a lawyer, operated widely-accessible websites to advertise the fraudulent scheme); United States v. Heckel, 570 F.3d 791, 792 (7th Cir. 2009) (enhancement upheld where defendant "used the Internet to conduct large-scale advertising to attract bidders to his fraudulent online auctions."); United States v. Pirello, 255 F.3d 728, 731 (9th Cir. 2001) (upholding mass-marketing enhancement in former §2F1.1: "By placing a classified ad on the Internet, Pirello was able to solicit funds instantaneously and continuously from over 200 million individuals worldwide."); *see also* United States v. Hanny, 509 F.3d 916, 920 (8th Cir. 2007) (upholding comparable mass-marketing enhancement in §2D1.1, stating, "[a] public,

c. Section 1037 offenses involving email addresses obtained through improper means

Section 2B1.1(b)(6) provides an additional increase specifically for section 1037 offenses. This 2-level increase applies whenever the defendant is convicted of an offense under 18 U.S.C. § 1037 and the offense involved obtaining email addresses through improper means.[69] Whereas application of most other SOCs in §2B1.1 are based on relevant conduct principles in §1B1.3 (Relevant Conduct (Factors that Determine the Guideline Range)), a defendant must be convicted of an offense under section 1037 for subsection (b)(6) to apply.[70] Pursuant to Application Note 6, "improper means" includes the unauthorized harvesting of email addresses of users of websites, proprietary services, or other public online forums.[71]

d. Sophisticated means

Computer crimes can involve a defendant's use of sophisticated means to commit the offense. Section 2B1.1(b)(10) requires a 2-level enhancement if:

> (A) the defendant relocated, or participated in relocating, a fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials;
>
> (B) a substantial part of a fraudulent scheme was committed from outside the United States; or
>
> (C) the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused conduct constituting sophisticated means.[72]

In addition, section (b)(10) establishes a minimum offense level of 12 in such cases.

Application Note 9(B) defines "sophisticated means" as "especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense," and provides examples of what constitutes sophisticated means, such as a

---

interactive website reachable by an ordinary web search engine is, at the least, a billboard on the information superhighway.").

69 USSG §2B1.1(b)(6).

70 *Id.*; *see also* USSG §1B1.3 (n.7) ("A particular guideline (in the base offense level or in a specific offense characteristic) may expressly direct that a particular factor be applied only if the defendant was convicted of a particular statute.").

71 USSG §2B1.1, comment. (n.6). The Fifth Circuit upheld an enhancement under subsection (b)(6) where the defendant was convicted under section 1037 and "dictionary attacks" were used to automatically generate email addresses "that are likely to belong to real people." United States v. Simpson, 796 F.3d 548, 555 (5th Cir. 2015). The court stated, "[the defendant] does not argue that dictionary attacks do not qualify as 'improper means' under the enhancement. We do note, however, that under the CAN-SPAM Act of 2003, it is unlawful to send e-mail to addresses obtained by a dictionary attack" before upholding the enhancement. *Id.*

72 USSG §2B1.1(b)(10).

telemarketing scheme involving locations in multiple jurisdictions or hiding assets through fictitious entities, corporate shells, or offshore financial accounts. [73] In addition, Application Note 9(C) states that the adjustment in §3C1.1 (Obstructing or Impeding the Administration of Justice) does not apply if the conduct that formed the basis for an enhancement under subsection (b)(10) (*e.g.*, conduct constituting sophisticated means) is the only conduct that forms the basis for the adjustment under §3C1.1.[74]

Courts look at the totality of the circumstances surrounding the scheme to determine whether the offense involved sophisticated means.[75] Courts have upheld the sophisticated means enhancement in cases involving (1) manipulation of computer systems and financial records;[76] (2) manufacturing items by computer to make schemes appear legitimate;[77] (3) acquisition of personal information through email accounts;[78] and (4) repeated access to protected computers or systems to obtain usernames and passwords.[79]

e. Device-making equipment and unauthorized access devices

Computer crimes that involve device-making equipment or unauthorized access devices may receive enhancements under §2B1.1(b)(11). Subsection (b)(11) provides for a 2-level increase if the offense involved:

---

[73] USSG §2B1.1, comment. (n.9(B)).

[74] USSG §2B1.1, comment. (n.9(C)).

[75] *See*, *e.g.*, United States v. Barrington, 648 F.3d 1178, 1199 (11th Cir. 2011) ("Even if each step in the scheme was not necessarily sophisticated, suffice it to say that the scheme as a whole used sophisticated means to obtain the unique usernames and passwords and access the Registrar's protected computer system."); United States v. Bistrup, 449 F.3d 873, 882 (8th Cir. 2006) ("Even if any single step is not complicated, repetitive and coordinated conduct can amount to a sophisticated scheme.").

[76] *See* United States v. Simmerman, 850 F.3d 829, 833 (6th Cir. 2017) (enhancement properly applied where defendant manipulated computer system and financial records, used fictitious identification numbers, created a dormant account, and structured her deposits to conceal offense).

[77] *See*, *e.g.*, United States v. Louper-Morris, 672 F.3d 539, 564–65 (8th Cir. 2012) (upholding enhancement where the defendant, among other things, prepared thousands of tax returns and power-of-attorney forms, endorsed with fraudulent signatures); United States v. Robinson, 538 F.3d 605, 607–08 (7th Cir. 2008) (enhancement upheld where defendant, among other things, used computer to manufacture counterfeit checks with legitimate bank routing and account numbers); United States v. Harvey, 413 F.3d 850, 853 (8th Cir. 2005) (upholding enhancement where defendants used computer to generate checks, along with other means to "make their transactions look legitimate").

[78] *See* United States v. Igboba, 964 F.3d 501, 507, 512 (6th Cir. 2020) (upholding enhancement where district court found "enhancement applied whether or not cryptocurrency was used in the offense and whether or not most of it happened in the United States," and "as signs of the offense's sophistication, [] highlighted Defendant's use of a VPN, Tor, the dark web, multiple bank accounts, and multiple email aliases to commit the crime, as well as the difficulty of acquiring taxpayer PII in the first place.").

[79] *Barrington*, 648 F.3d at 1199 (upholding the enhancement where the defendant "repeatedly accessed [a] protected computer grading system using log-in information retrieved through [] keyloggers [and] [t]he hacking involved multiple, repetitive and coordinated steps to deceive and exploit [the] protected system").

(A) possession or use of any device-making equipment or authentication feature;

(B) production or trafficking of any unauthorized access device or counterfeit access device, or authentication feature; or

(C) unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification, or possessing five or more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification.[80]

Subsection (b)(11) also establishes a minimum offense level of 12.[81]

The term "device-making equipment" has the meaning given the term in 18 U.S.C. § 1029(e)(6): "any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device."[82] The Commentary to §2B1.1 also provides that such term includes scanning receivers and hardware or software 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."[83] Depending on the circumstances, the term "device-making equipment" may include keylogger software or computers equipped with digital templates for state identification cards.[84]

---

[80] USSG §2B1.1(b)(11). For defendants convicted of violating 18 U.S.C. § 1028A and sentenced under §2B1.6 (Aggravated Identity Theft), the guideline sentence is the term of imprisonment required by statute (Chapters Three and Four do not apply to that count of conviction). USSG §2B1.6(a). If a sentence under §2B1.6 is imposed in conjunction with a sentence for an underlying offense (which commonly occurs with offenses sentenced under §2B1.1), any SOC for the transfer, possession, or use of a means of identification, such as those listed in §2B1.1(b)(11)(C), do not apply when determining the sentence for the underlying offense. USSG §2B1.6, comment. (n.2). Section §2B1.6 already accounts for those factors. *Id.*

[81] USSG §2B1.1(b)(11); *see also* USSG §2B1.1, comment. (backg'd) ("This subsection provides a minimum offense level of level 12, in part because of the seriousness of the offense. The minimum offense level accounts for the fact that the means of identification that were 'bred' (*i.e.*, produced or obtained) often are within the defendant's exclusive control, making it difficult for the individual victim to detect that the victim's identity has been 'stolen.' . . . . The minimum offense level also accounts for the non-monetary harm associated with these types of offenses, much of which may be difficult or impossible to quantify (*e.g.*, harm to the individual's reputation or credit rating, inconvenience, and other difficulties resulting from the offense).").

[82] USSG §2B1.1, comment. (n.10(A)); 18 U.S.C. § 1029(e)(6).

[83] USSG §2B1.1, comment. (n.10(A)); 18 U.S.C. § 1029(a)(9). For purposes of §2B1.1, a "scanning receiver" is one referred to in 18 U.S.C. § 1029(a)(8) ("knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver") and such term has the meaning given in 18 U.S.C. § 1029(e)(8) ("a device or apparatus that can be used to intercept a wire or electronic communication in violation of chapter 119 [of title 18, United States Code] or to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument."). USSG §2B1.1, comment. (n.10(A)).

[84] USSG §2B1.1, comment. (n.10); 18 U.S.C. § 1029(a)(9); *see also* United States v. Jones, 792 F.3d 831, 835–36 (7th Cir. 2015) ("Jones possessed device-making equipment—his computer equipped with state identification templates—and he used that equipment to produce fake IDs for his writers."); United States v. Barrington, 648 F.3d 1178, 1202 (11th Cir. 2011) ("[T]he record evidence sufficiently supports a finding that

"Unauthorized access device" has the meaning given the term in 18 U.S.C. § 1029(e)(3), which is "any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud."[85] Social security numbers, usernames, and passwords may qualify as unauthorized access devices.[86]

f. Section 1030 offenses involving personal information and substantial disruption of critical infrastructures

Section 2B1.1 includes two enhancements that involve 18 U.S.C. § 1030 offenses—subsections (b)(18) and (b)(19), which take into account characteristics of computer crimes that may not be fully captured in a loss calculation, such as an invasion of privacy or disruption to a critical infrastructure.[87] As such, if the offense of conviction is under section 1030, subsections (b)(18) and (b)(19) may apply in addition to all other applicable SOCs in §2B1.1.

---

keyloggers constitute device-making equipment as defined in 18 U.S.C. § 1029(e)(6). However, the district court apparently based its conclusion that the keylogger software constituted device-making equipment on the finding that the keylogger software constituted a 'scanning receiver.' . . . We do not believe this finding is adequately supported by the record."). *But see* United States v. Tatum, 518 F.3d 769, 772 n.5 (10th Cir. 2008) (leaving unresolved defendant's argument that computer and scanner used to create counterfeit checks did not constitute "device-making equipment" because each device is "not primarily used to commit crimes" but noting two circuits have "adopted a middle ground in construing the definition of device-making equipment . . . ." (citing United States v. Cabrera, 208 F.3d 309 (1st Cir. 2000) and United States v. Morris, 81 F.3d 131 (11th Cir. 1996))).

[85] USSG §2B1.1, comment. (n.10(A)); 18 U.S.C. § 1029(e)(3). Section 1029(e)(1) defines "access device" as "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification 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 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)." 18 U.S.C. § 1029(e)(1).

[86] *See* United States v. Wright, 862 F.3d 1265, 1275 (11th Cir. 2017) (social security number qualifies as an "access device" for purposes of the definition in 18 U.S.C. § 1029(e) and the sentencing guidelines); *Barrington*, 648 F.3d at 1202 (obtaining usernames and passwords with intent to defraud renders them "unauthorized access devices" as defined in section 1029(e)(3)).

[87] *See* USSG App. C, amend. 654 (effective Nov. 1, 2003) ("This amendment addresses the serious harm and invasion of privacy that can result from offenses involving the misuse of, or damage to, computers."). Through amendment 654, the Commission, among other things, added the enhancement found in §2B1.1(b)(19) and an initial version of the enhancement found in §2B1.1(b)(18) following the directives in the Cyber Security Enhancement Act of 2002, Pub. L. No. 107–296, § 225, 116 Stat. 2150. The Act contained a directive for the Commission to review the sentencing guidelines relating to section 1030 offenses and consider eight factors: (1) the potential and actual loss; (2) the level of sophistication and planning; (3) whether commercial advantage or private financial benefit was involved; (4) whether malicious intent to cause harm existed; (5) the extent of the harm to individual privacy rights; (6) whether the offense involved a computer used by the government in furtherance of national defense or security, or the administration of justice; (7) whether substantial disruption or interference of a critical infrastructure was intended or effectuated; and (8) whether public health or safety, or injury to a person, was intended or effectuated. *Id.* § 225. The Commission issued a Report to the Congress explaining its amendments and recommendations in response to the congressional directives. *See* 2003 REPORT TO CONGRESS ON CYBER SECURITY OFFENSES, *supra* note 26.

First, subsection (b)(18) provides for a 2-level increase "[i]f (A) the defendant was convicted of an offense under 18 U.S.C. § 1030, and the offense involved an intent to obtain personal information, or (B) the offense involved the unauthorized public dissemination of personal information."[88] Each subparagraph of the enhancement in §2B1.1(b)(18) targets different harms.[89] For purposes of subparagraph (A), the enhancement applies if the defendant has been convicted of an offense under 18 U.S.C. § 1030 and the offense involved an intent to obtain personal information.[90] In contrast, subparagraph (B) does not require a conviction under any specific statute but applies to any offense that involves the unauthorized public dissemination of personal information.[91] The Commentary defines "personal information" as "sensitive or private information involving an identifiable individual (including such information in the possession of a third party)" and includes medical records, private correspondence (including email), financial records, private photographs, or similar information.[92]

Second, like subsection (b)(18)(A), subsection (b)(19)(A) is offense-specific and requires a conviction under 18 U.S.C. § 1030. Pursuant to subsection (b)(19)(A), the court applies the greatest applicable increase of the following: a 6-level increase if the defendant was convicted under section 1030 and the offense caused a substantial disruption of a critical infrastructure; a 4-level increase if the defendant was convicted under section 1030(a)(5)(A) (*i.e.*, "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"); or a 2-level increase if the defendant was convicted of an offense under section 1030 and the offense involved a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security.[93] "Critical infrastructure" is defined as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters."[94]

---

88 USSG §2B1.1(b)(18).

89 As stated above, a version of subsection (b)(18) was added to what is now §2B1.1(b)(19)(A) in response to the Cyber Security Enhancement Act in 2003. In 2009, the Commission, in response to the Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110–326, § 209, 122 Stat. 3564, separated the text relating to personal information from the graduated list and expanded it to address harms created by all offenses sentenced under §2B1.1 that involve personal information. *See* USSG App. C, amend. 726 (effective Nov. 1, 2009) ("Moving the intent to obtain personal information prong out of the computer crime enhancement and into the new enhancement ensures that a defendant convicted under section 1030 receives an incremental increase in punishment if the offense involved both an intent to obtain personal information and another harm addressed by the computer crime enhancement. The '(B)' prong of the new personal information enhancement ensures that any defendant, regardless of the statute of conviction, receives an additional incremental increase in punishment if the offense involved the unauthorized public dissemination of personal information. This prong accounts for the greater harm to privacy caused by such an offense.").

90 USSG §2B1.1(b)(18)(A).

91 USSG §2B1.1(b)(18)(B); *see also* USSG §§1B1.1, 1B1.3.

92 USSG §2B1.1, comment. (n.1).

93 USSG §2B1.1(b)(19)(A).

94 USSG §2B1.1, comment. (n.15(A)).

A "critical infrastructure" may be publicly or privately owned and includes telecommunications networks, banking systems, emergency services, and transportation services.[95]

Subsection (b)(19)(B) establishes a minimum offense level of 24 if the 6-level increase in subsection (b)(19)(A)(iii) applies, which reflects "the serious impact such an offense could have on national security, national economic security, national public health or safety, or a combination of any of these matters."[96] In addition, if the 6-level increase applies and the disruption is so substantial as to have a "debilitating" impact on national security, national economic security, public health or safety, or any combination of these matters, an upward departure would be warranted.[97]

g. Departures

Section 2B1.1 is designed to capture pecuniary harm, the most common harm in a fraud case. However, the Commission recognized that, in some cases, harm to the victims for offenses sentenced under §2B1.1 goes beyond monetary losses.[98] For example, §2B1.1 includes departure provisions for the court to consider for all fraud offenses (including computer fraud) if, for example, (1) a primary objective of the offense was an aggravating, non-monetary objective; (2) the offense resulted in a substantial invasion of a privacy interest; or (3) the offense involved stolen information from a protected computer to further a broader criminal purpose.[99]

For all cases sentenced under §2B1.1, Application Note 21(A) states that an upward departure may be warranted if the defendant's offense level determined under §2B1.1

---

95 *Id.*

96 USSG §2B1.1(b)(19)(B) and comment. (backg'd.). The Fifth Circuit held that a district court erred in applying the 6-level increase and minimum offense level for substantial disruption of a critical infrastructure where the defendant, in intentionally damaging a protected computer, caused Citibank "relatively minor financial losses" and a temporary disruption in service. United States v. Brown, 884 F.3d 281, 287 (5th Cir. 2018).

97 USSG §2B1.1, comment. (n.21(B)).

98 *See*, *e.g.*, USSG App. C, amend. 551 (effective Nov. 1, 1997) (adding, among other things, upward departure for cases where a defendant convicted of theft from protected computer "sought stolen information to further a broader criminal purpose"); USSG App. C, amend. 596 (effective Nov. 1, 2000) ("The minimum offense level also accounts for the non-monetary harms associated with identity theft (*e.g.*, harm to reputation or credit rating), which typically are difficult to quantify. However, for cases in which the nature and scope of the harm to an individual victim is so egregious that the two-level enhancement and minimum offense level provide insufficient punishment, the amendment invites an upward departure.").

99 USSG §2B1.1, comment. (n.21(A)(i), (ii), & (v)). Section 2B1.1 includes multiple departure provisions in its commentary, one in Application Note 8(A) and several in Application Note 21, for the court to consider based on the facts of the case at hand. This section covers the departures in §2B1.1 that commonly apply to computer fraud cases and that capture certain factors that are often present in computer crimes. For more information on departures generally, see U.S. SENT'G COMM'N, PRIMER ON DEPARTURES AND VARIANCES (2021), https://www.ussc.gov/guidelines/primers/departures-and-variances.

substantially understates the seriousness of the offense.[100] Application Note 21(A) then provides a non-exhaustive list of factors the court may consider in determining whether a departure is warranted for all types of fraud offenses,[101] including cases that involved "protected computers," access devices, and unlawfully obtained means of identification.[102]

Among the factors included in Application Note 21, under subparagraph (A)(ii), the court may also consider whether an upward departure is warranted if the offense caused or risked substantial non-monetary harm. For example, an upward departure would be warranted under this factor if death results from a section 1030 offense involving damage to a protected computer.[103] Under subparagraph (A)(v), courts may consider departing upward in cases involving stolen information from protected computers if the information sought furthered a broader criminal purpose.[104] In addition, under subparagraph (A)(vi), courts may consider departing upward in cases involving access devices or unlawfully produced or obtained means of identification if:

> (I) The offense caused substantial harm to the victim's reputation, or the victim suffered a substantial inconvenience related to repairing the victim's reputation.
>
> (II) An individual whose means of identification the defendant used to obtain unlawful means of identification is erroneously arrested or denied a job because an arrest record has been made in that individual's name.
>
> (III) The defendant produced or obtained numerous means of identification with respect to one individual and essentially assumed that individual's identity.[105]

Subparagraphs (C) and (D) of Application Note 21 provide that a downward departure may be warranted in cases where the offense level determined under §2B1.1 substantially

---

[100] USSG §2B1.1, comment. (n.21(A)).

[101] For example, Application Note 21(A) provides, for all fraud cases, the following for the court to consider in determining whether an upward departure is warranted: a primary objective of the offense was an aggravating, non-monetary objective (such as inflicting emotional harm); the offense caused or risked substantial non-monetary harm (including physical, psychological, or emotional trauma, or invasion of privacy); the offense involved substantial amounts of interest, penalties, or other costs; or the offense created a risk of substantial loss (such as risk of a significant disruption of a national financial market). USSG §2B1.1, comment. (n.21(A)(i)–(iv)).

[102] USSG §2B1.1, comment. (n.21(A)(v)–(vi)).

[103] USSG §2B1.1, comment. (n.21(A)(ii)).

[104] USSG §2B1.1, comment. (n.21(A)(v)); *see also* United States v. Rodriguez, 443 F. App'x 504, 509–10 (11th Cir. 2011) (per curiam) (7-level upward departure upheld where district court considered factors in upward departure provision and defendant's "broader criminal purpose" in obtaining medical records from protected computer was to receive kickbacks from referrals to personal injury lawyers and clinics).

[105] USSG §2B1.1, comment. (n.21(A)(vi)).

overstates the seriousness of the offense or in cases involving defendants that sustained damage, loss, hardship, or suffering caused by a major disaster or an emergency.[106]

IV. TRESPASSING ON A GOVERNMENT COMPUTER

A. Relevant Statute: 18 U.S.C. § 1030(a)(3) (Trespassing on a Government Computer)

Section 1030(a)(3) criminalizes intentional unauthorized access to any nonpublic computer of a department or agency of the United States that is exclusively for the use of the United States government, or if not exclusively for such use, is used by or for the United States government and the conduct affects such use.[107] Offenses under section 1030(a)(3) are punishable by not more than one year in prison unless the defendant has a prior conviction for an offense under section 1030, in which case the statutory maximum is ten years of imprisonment.[108]

B. Applicable Guideline: Section 2B2.3 (Trespass)

The applicable guideline for offenses under section 1030(a)(3) is §2B2.3 (Trespass).[109] Section 2B2.3 has a base offense level of 4, three SOCs, and one cross reference. Two of the three SOCs directly involve computer crimes.[110] First, subsection (b)(1) provides for offense level increases if the trespasses occurs on or to certain property, including a 2-level increase for trespassing on computer systems used to maintain or operate a critical infrastructure or used by or for a government entity in furtherance of the administration of justice, national defense, or national security.[111] Application Note 1 defines "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters."[112]

---

106 USSG §2B1.1, comment. (n.21(C)–(D)).

107 18 U.S.C. § 1030(a)(3).

108 *Id.* § 1030(c)(2)(A), (C).

109 USSG App. A.

110 The SOC that does not directly involve computers is the 2-level increase for possession of a dangerous weapon in USSG §2B2.3(b)(2).

111 USSG §2B2.3(b)(1). Subsection (b)(1) provides for a 4-level increase if the trespass occurs at the White House or at the Vice President's official residence, otherwise, a 2-level increase applies under this subsection. The Commission promulgated subsection (b)(1)(A)(viii), for trespassing on a computer system, to expand the scope of the enhancements in §2B2.3 to ensure that computer crimes are addressed. *See* USSG App. C, amend. 654 (effective Nov. 1, 2003).

112 USSG §2B2.3, comment. (n.1). A "critical infrastructure" may be publicly or privately owned and includes telecommunications networks, banking systems, emergency services, and transportation services. *Id.*

Next, subsection (b)(3) provides an increase of one or more levels (consistent with the increase in levels in the §2B1.1 loss table) if the offense involved invasion of a protected computer and the resulting loss exceeded $2,500.[113] The court determines loss, for purposes of §2B2.3(b)(3), pursuant to the rules for the determination of loss in the Commentary to §2B1.1.[114] For purposes of §2B2.3, "protected computer" means a computer described in 18 U.S.C. § 1030(e)(2).[115]

The guideline also includes a cross reference, which instructs that if the trespass offense was committed with the intent to commit a felony offense (such as an assaultive offense or a murder) that would have a resulting offense level greater than the one determined under §2B2.3, the court applies §2X1.1 (Attempt, Solicitation, or Conspiracy).[116]

V. EXTORTION INVOLVING PROTECTED COMPUTERS

A. RELEVANT STATUTE: 18 U.S.C. § 1030(A)(7) (EXTORTION INVOLVING PROTECTED COMPUTERS)

Section 1030(a)(7) prohibits extortion involving protected computers. A person commits an offense under section 1030(a)(7) if, with intent to extort another, he or she transmits into interstate commerce any communication containing (1) a threat to cause damage to a protected computer; (2) a threat to obtain information from a protected computer without authorization (or exceeding authorized access) or to impair confidentially of such information; or (3) a demand for something of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.[117] A defendant faces up to five years of imprisonment for a violation of section 1030(a)(7) unless the defendant has a prior conviction for a section 1030 offense, in which case the statutory maximum punishment is ten years.[118]

[113] USSG §2B2.3(b)(3); *see also* USSG App. C, amend. 551 (effective Nov. 1, 1997) ("This amendment makes a number of changes in the theft, property destruction, trespass, extortion, and fraud guidelines to more effectively punish computer-related offenses.").

[114] USSG §2B2.3, comment. (n.2); *see* discussion *supra* Section III.B.2.a. For a guide to determining loss generally, see LOSS CALCULATIONS PRIMER, *supra* note 54.

[115] USSG §2B2.3, comment. (n.1); *see supra* text accompanying note 15. The Commentary further incorporates the statutory definition of a "government entity" by reference to 18 U.S.C. § 1030(e)(9). *See id.*

[116] USSG §2B2.3(c).

[117] 18 U.S.C. § 1030(a)(7). A "protected computer" is defined in section 1030(e)(2). *See supra* text accompanying note 15.

[118] 18 U.S.C. § 1030(c)(3).

B. Applicable Guideline: Section 2B3.2 (Extortion by Force or Threat of Injury or Serious Damage)

Offenses under section 1030(a)(7) are referenced in Appendix A to §2B3.2.[119] Section 2B3.2 has a base offense level of 18, five SOCs, and two cross references.[120]

The SOCs in §2B3.2 provide offense level increases for a variety of aggravating circumstances, such as death threats, bodily injury, kidnapping, and loss.[121] Directly related to computers, the SOC in subsection (b)(3)(B)(i)(V)[122] provides for a 3-level increase if the offense involved preparation, or a demonstrated ability, to carry out threats of damage to a computer system used to maintain or operate a critical infrastructure, or used by or for a government entity in furtherance of the administration of justice, national defense, or national security.[123]

The Commentary defines "critical infrastructure" as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters."[124] A "critical infrastructure" may be publicly or privately owned and includes telecommunications networks, banking systems, emergency services, and transportation services.[125] The Commentary further incorporates the statutory definition of a "government entity" by reference to 18 U.S.C. § 1030(e)(9), which states that the term includes the United States government, its states and political subdivisions, and foreign countries and their states, provinces, municipalities, or political subdivisions.[126]

---

[119] USSG App. A.

[120] USSG §2B3.2(a)–(c). This section discusses one of the five SOCs in detail because it relates to computer crimes specifically. The guideline includes two cross references, one to §2A1.1 (First Degree Murder) if a victim was killed under circumstances that would constitute murder and another to §2A2.1 (Assault with Intent to Commit Murder; Attempted Murder) if the offense was tantamount to attempted murder and the resulting offense is greater than determined under §2B3.2. USSG §2B3.2(c).

[121] USSG §2B3.2(b)(1), (b)(2), (b)(4), and (b)(5).

[122] Section 2B3.2(b)(3) provides alternative increases based upon (A) whether a firearm was discharged, used, brandished, or possessed or a dangerous weapon was used, brandished, or possessed, or (B) whether the offense involved preparation to carry out certain threats, such as death, serious bodily injury, kidnapping, product tampering, or damage to certain computer systems, or if the participant otherwise demonstrated the ability to carry out a threat of same. USSG §2B3.2(b)(3). The alternative increases in subsection (b)(3)(B) account for aggravating circumstances that do not involve weapons but are similarly serious. *See* USSG §2B3.2, comment. (n.6) ("In certain cases, an extortionate demand may be accompanied by conduct that does not qualify as a display of a dangerous weapon under subsection (b)(3)(A)(v) but is nonetheless similar in seriousness . . . . Subsection (b)(3)(B) addresses such cases.").

[123] USSG §2B3.2(b)(3)(B)(i)(V). The Commission added this enhancement following the directives in the Homeland Security Act of 2002, thereby expanding the existing enhancements to account for offenses involving computer systems used to maintain or operate critical infrastructures. *See* USSG App. C, amend. 654 (effective Nov. 1, 2003); *see also* 2003 Report to Congress on Cyber Security Offenses, *supra* note 26, at 5–6.

[124] USSG §2B3.2, comment. (n.1).

[125] *Id.*

[126] *Id.*; 18 U.S.C. § 1030(e)(9).

VI. CHAPTER THREE ADJUSTMENTS: SECTION 3B1.3 AND COMPUTERS

Chapter Three adjustments often apply to computer crimes. This section of the primer focuses on the adjustment in §3B1.3 (Abuse of Position of Trust or Use of Special Skill); however, courts have also analyzed other Chapter Three adjustments in cases involving computers, such as those for vulnerable victim (§3A1.1), terrorism (§3A1.4), aggravating role (§3B1.1), mitigating role (§3B1.2), and obstruction of justice (§3C1.1).[127]

Section 3B1.3 provides a 2-level adjustment if the defendant abused a position of trust or used a special skill that significantly facilitated the commission or concealment of the offense, both of which could apply to computer crimes. The government must prove the adjustment applies by a preponderance of the evidence.[128] The adjustment does not apply if an abuse of trust or special skill is included in the base offense level or SOC.[129]

A. ABUSE OF POSITION OF TRUST

Section 3B1.3 provides for an adjustment if the defendant abuses a position of public or private trust that significantly facilitates the commission or concealment of the offense.[130] "Public or private trust" refers to a position that characterized by professional or managerial discretion (*i.e.*, substantial discretionary judgment that is ordinarily given considerable deference). For the adjustment to apply, the position of trust must have contributed in a significant way to facilitating the commission or concealment of the offense.[131] The adjustment applies even if the position of trust is fictitious.[132] In addition,

[127] *See, e.g.*, United States v. Sunmola, 887 F.3d 830, 837–39 (7th Cir. 2018) (in a case involving an online dating scam, upholding the vulnerable victim adjustment where defendants targeted "divorced, abandoned, widowed, or ignored" women seeking companionship and the aggravating role adjustment where defendant "recruited accomplices, placed the orders for merchandise . . . acquired the phony credit card data used to make the purchases . . . and directed everyone else on what to tell the victims."); United States v. Wright, 862 F.3d 1265, 1278 (11th Cir. 2017) (defendant did not meet burden of proving minor role because evidence showed she kept personal identifying information (PII) for thousands of people in her home, on her phone, and on her computer, and texted that information to others); United States v. King, 604 F.3d 125, 141–42 (3d Cir. 2010) (defendant received obstruction adjustment because "he destroyed three hard drives containing evidence and taught [another] how to destroy a computer's hard drive."); United States v. Hale, 448 F.3d 971, 988 (7th Cir. 2006) (per curiam) (upholding terrorism adjustment where defendant used internet chat rooms and emails to locate and publish judge's address and solicit murder).

[128] *See*, *e.g.*, United States v. Zehrung, 714 F.3d 628, 630 (1st Cir. 2013); United States v. Miell, 661 F.3d 995, 998 (8th Cir. 2011).

[129] USSG §3B1.3; *see*, *e.g.*, USSG §§2A3.3, 2C1.2, and 2H1.1.

[130] USSG §3B1.3.

[131] USSG §3B1.3, comment. (n.1).

[132] USSG §3B1.3, comment. (n.3) ("This adjustment also applies in a case in which the defendant provides sufficient indicia to the victim that the defendant legitimately holds a position of private or public trust when, in fact, the defendant does not."); *see also* USSG App. C, amend. 580 (effective Nov. 1, 1998) (resolving a circuit split on the issue, stating, "The Commission has determined that, particularly from the perspective of the crime victim, an imposter who falsely assumes and takes advantage of a position of trust is as culpable and deserving of increased punishment as is a defendant who abuses an actual position of trust.").

the adjustment applies if the defendant abused his or her authority to obtain, transfer, issue unlawfully, or use without authorization, any means of identification.[133] The Commentary provides examples of appropriate application of the adjustment.[134]

In applying the abuse of position of trust adjustment, the majority of circuit courts employ a two-part approach that tracks the guideline: courts first look to whether the defendant held a position of trust, and, if so, the court decides whether the defendant used the position to significantly facilitate or conceal the offense.[135] Using this two-part test, the

[133] USSG §3B1.3, comment. (n.2); United States v. Cruz, 713 F.3d 600, 608–09 (11th Cir. 2013) ("By abusing the authority of her position at Target to help her co-conspirators use credit cards without authorization, and indirectly using a means of identification without authority herself by using the products of identity theft for personal gain, [the defendant] committed conduct that application note 2(B) to § 3B1.3 prohibits."). In this type of case, the adjustment applies regardless of whether the defendant would qualify under the definition in Application Note 1. *Id.*; *see also* USSG App. C, amend. 677 (effective Nov. 1, 2005) (implementing Identity Theft Penalty Enhancement Act, Pub. L. No. 108–275, 118 Stat. 831 (2004), which created two new criminal offenses at 18 U.S.C. § 1028A and directed the Commission to expand the adjustment in §3B1.3 to apply to defendants who exceed or abuse their authority in order to obtain unlawfully or use without authority any means of identification); United States v. Godsey, 690 F.3d 906, 910 (8th Cir. 2012) (upholding adjustment under §3B1.3 where the district court did not first establish whether the defendant occupied a "position of public or private trust" holding that Application Note 2's "own terms sever it from other § 3B1.3 requirements . . . . [a]ccordingly, we find that Application Note 2(B) is an independent basis for applying an adjustment under § 3B1.3.").

[134] *See*, *e.g.*, USSG §3B1.3, comment. (n.1) (listing examples on the general applicability of the adjustment), (n.2(B)) (listing examples involving means of identification), and (n.3) (listing examples involving imposters). Application Note 5 illustrates how an adjustment for abuse of trust may apply in cases involving theft or embezzlement from labor unions or employee pension or welfare benefit plans. USSG §3B1.3, comment. (n.5).

[135] *See, e.g.*, United States v. Alston, 899 F.3d 135, 151 (2d Cir. 2018), *cert. denied*, 139 S. Ct. 1282 (2019); United States v. Miell, 661 F.3d 995, 998 (8th Cir. 2011); United States v. Guidry, 199 F.3d 1150, 1159–60 (10th Cir. 1999). At least seven circuits analyze whether the defendant held a position of trust from the perspective of the victim. *See, e.g.*, United States v. George, 841 F.3d 55, 67 (1st Cir. 2016); *Alston*, 899 F.3d at 151 (citing United States v. Huggins, 844 F.3d 118, 124 (2d Cir. 2016)); United States v. Thomsen, 830 F.3d 1049, 1073–74 (9th Cir. 2016); United States v. Demarco, 784 F.3d 388, 397 (7th Cir. 2015); United States v. Abdelshafi, 592 F.3d 602, 611 (4th Cir. 2010); Payne v. United States, 566 F.3d 1276, 1277 (11th Cir. 2009) (per curiam); *Guidry*, 199 F.3d at 1160. *But see* United States v. Buck, 324 F.3d 786, 794 (5th Cir. 2003) ("We have never held . . . nor do the guidelines explicitly require, that the determination . . . must be assessed from the perspective of the victim.").

The Sixth Circuit narrows the application of §3B1.3 by requiring that (1) the defendant abused the position of trust specifically with the victim of the offense charged, and (2) the "decisive factor" is the level of discretion given to an employee. *See* United States v. May, 568 F.3d 597, 603 (6th Cir. 2009) ("Our case law has also constrained the circumstances under which the abuse-of-trust enhancement can apply."); United States v. Ragland, 72 F.3d 500, 503 (6th Cir. 1996) (vacating §3B1.3 adjustment because the defendant's "position was not characterized by substantial discretionary judgment that is ordinarily given considerable deference. In fact, she was not authorized to exercise any meaningful discretion."). The Sixth Circuit upheld the adjustment for a credit union manager who manipulated and diverted monies using a computer program normally used for tracking it within the credit union. United States v. Simmerman, 850 F.3d 829, 831–32, 835–36 (6th Cir. 2017). Conversely, it reversed and remanded a sentence where the defendant's position as an assistant treasurer was similar to a "computer programmer or technician" rather than one indicating a position of trust. United States v. Brogan, 238 F.3d 780, 783–86 (6th Cir. 2001).

Fifth Circuit in *United States v. Miller*[136] upheld application of the adjustment where the defendant, an accounts payable clerk, used her position to use company accounting software to manipulate bookkeeping and print fraudulent checks. The Eleventh Circuit, using this approach in *United States v. Pedersen*,[137] upheld the adjustment in a case involving a Chicago police detective who unlawfully accessed and disclosed confidential information (and recruited others to do so) from the National Crime Information Center (NCIC) database to a corporation that sold the information to employers, insurance companies, and investigators.

B. USE OF SPECIAL SKILL

If the defendant uses a special skill that significantly facilitates the commission or concealment of the offense, the 2-level adjustment in §3B1.3 may apply.[138] Unlike the abuse of trust adjustment, an adjustment solely for the use of a special skill may not be applied in addition to an adjustment under §3B1.1 (Aggravating Role).[139] The guidelines define a "special skill" as one not possessed by the general public and that usually requires substantial education, training, or licensing.[140] The Seventh Circuit upheld the adjustment

[136] 906 F.3d 373, 377–79 (5th Cir. 2018). The court found that substantial discretion, little supervision, autonomy, and knowledge of the accounting procedures significantly facilitated the fraud. *Id.* at 378.

[137] 3 F.3d 1468, 1471–72 (11th Cir. 1993). Some circuits that require the two-part test have considered additional factors, such as the nature of the relationship between the parties, responsibilities, and any special access granted to the defendant based upon his or her position of trust. *See, e.g.*, *Miller*, 906 F.3d at 377–78; *DeMarco*, 784 F.3d at 397; United States v. Laurienti, 731 F.3d 967, 973 (9th Cir. 2013); *Abdelshafi*, 592 F.3d at 610–11; United States v. Ghertler, 605 F.3d 1256, 1264 (11th Cir. 2010).

In a recent *en banc* decision, the Third Circuit "refined" its analysis under §3B1.3 to direct district courts to additionally consider a series of factors during each step of their determination. United States v. Douglas, 885 F.3d 124, 132–34 (3d Cir. 2018) (en banc). The court noted that its decision did not necessarily overrule its prior precedent relating to the adjustment. *See id.* at 133 n.5. One such example of a pre-*Douglas* case involving computer crimes is illustrated in an unpublished opinion, where the Third Circuit upheld the adjustment for a systems administrator who installed and used a "logic bomb" on his former employer's computer system. United States v. Duronio, No. 06-5116, 2009 WL 294377, at *3 (3d Cir. Feb. 9, 2009). In another case, the court upheld the adjustment for a claims processor who logged onto a state database using his supervisors' passwords. United States v. Lofink, 564 F.3d 232, 242 n.20 (3d Cir. 2009).

[138] USSG §3B1.3.

[139] *Id.*

[140] USSG §3B1.3, comment. (n.4) (listing lawyers, pilots, doctors, accountants, chemists, and demolition experts as examples). The D.C. Circuit has held that the special skills adjustment requires employment of "a pre-existing, legitimate skill not possessed by the general public[.]" United States v. Young, 932 F.2d 1510, 1513–15 (D.C. Cir. 1991). Courts differ in approach regarding what qualifies as "use" of the special skill. *See, e.g.*, United States v. Ramirez, 724 F. App'x 704, 719 (11th Cir. 2018) ("[The defendant] asks us to adopt the approach used by the Sixth Circuit in United States v. Weinstock, 153 F.3d 272 (6th Cir. 1998), and to differentiate between his status as a chiropractor and using his skills as one . . . . To the contrary, the government asks us to adopt the Third Circuit's approach from United States v. Tai, 750 F.3d 309 (3d Cir. 2014), which views the use of a special skill as including any action that requires the 'skill and credentials [as] the means by which [a defendant] could participate' . . . . We adopt the Sixth Circuit's approach . . . [o]ur reading of the word 'use' does not by its plain language include refraining from the use of one's skills.") (citations omitted).

where the defendant had an associate's degree in graphic design, specialized knowledge, and the ability to manipulate drawings in AutoCAD and used those skills to steal data and attempt to sell it to his former employer's competitors.[141] The Eleventh Circuit upheld the adjustment where the defendant had "skills in civil engineering, radio technology, and computer technology . . . legitimate skills [he] turned to criminal purposes."[142] The First Circuit upheld the adjustment where the defendant, a computer consultant, had special knowledge of an airline reservations program and trained others within a travel agency on that program.[143]

Courts have upheld the special skills adjustment in §3B1.3 in computer crimes cases where the defendant had no formal training or where the defendant's special knowledge is self-taught. For example, the Second Circuit upheld an adjustment where the defendant, with no special training in electronics, installed electronic equipment into ATMs that allowed him to access account numbers and withdraw money.[144] The First Circuit upheld an adjustment for a defendant who possessed computer skills that were self-taught and hacked into website order logs, rewrote scripts, and downloaded validity checks for credit card numbers to further access device fraud.[145]

In a case involving computer fraud and conspiracy to commit computer and wire fraud, the Ninth Circuit addressed in detail self-taught knowledge of computer systems and the use of that knowledge to facilitate an offense.[146] First, the court upheld the district court's application of the adjustment based upon the defendant's "extraordinary knowledge" of computers.[147] In a footnote, however, the court cautioned that, "[o]nly where a defendant's computer skills are *particularly sophisticated* do they correspond to the Sentencing Commission's examples of 'special skills'—lawyer, doctor, pilot, etc. . . . Courts should be particularly cautious in imposing special skills adjustments where substantial education, training or licensing is not involved."[148]

---

141 United States v. Lange, 312 F.3d 263, 270 (7th Cir. 2002).

142 United States v. Campa, 529 F.3d 980, 1017–18 (11th Cir. 2008) (case involving agents of the Cuban Directorate of Intelligence convicted of espionage and conspiracy to commit murder).

143 United States v. O'Brien, 435 F.3d 36, 42 (1st Cir. 2006); *see also, e.g.*, United States v. Kyereme, 371 F. App'x 292, 293–94 (3d Cir. 2010) (defendant possessed special skill where he held several degrees and professional licenses, "completed numerous computer and network training courses . . . [and] has been employed in the IT field since 1991.").

144 United States v. Lavin, 27 F.3d 40, 41 (2d Cir. 1994) (per curiam) (district court-imposed enhancement for use of "impressive knowledge of electronics").

145 United States v. Prochner, 417 F.3d 54, 61 (1st Cir. 2005) ("[A] court can reasonably infer requisite self-education from the nature and extent of the skill possessed.").

146 United States v. Petersen, 98 F.3d 502 (9th Cir. 1996). The offenses of conviction were computer fraud, possession of a stolen vehicle, conspiracy to commit computer and wire fraud, and interception of communications. *Id.* at 504.

147 *Id.* at 506–07.

148 *Id.* at 507 n.5 (emphasis added) (citation omitted). Later, the Ninth Circuit cited this footnote to distinguish the circumstances in the case at hand from those of the defendant in *Peterson*. United States v. Lee,

Other circuits have noted the above language in *Peterson* while analyzing, comparing, and contrasting courts' application of the "special skill" adjustment in cases involving computer crimes. For example, the Sixth Circuit noted then followed the language in *Peterson* before reversing the defendant's case for resentencing and finding that his use of Adobe Page Maker and a computer scanner to create counterfeit currency "can be duplicated by members of the general public with a minimum of difficulty."[149] In *United States v. Lord*,[150] a case involving failure to register a bitcoin[151] business and drug conspiracy, the Fifth Circuit noted the language, stating that one defendant did not "come close to the 'expert hacker' in *Petersen*" and lacked education, training, or licensing in the skills at issue—even though the defendant was described as "a very intelligent computer skills set-type person" that had a working knowledge of the "darknet[152] marketplace."[153]

296 F.3d 792, 797–99 (9th Cir. 2002). In *Lee*, the defendant created a website identical to the Honolulu marathon's website, registered a similar domain name, and sold fake registrations for the race. The Ninth Circuit reversed the district court's imposition of the special skills adjustment, citing the footnote in *Peterson*, because the defendant was "a video rental store operator who copied a website . . . . [whose] level of sophistication was nothing like Petersen's." *Id.* at 799.

149 United States v. Godman, 223 F.3d 320, 322–23 (6th Cir. 2000) ("Godman's computer skills thus are not 'particularly sophisticated' as suggested by the *Petersen* case."). Later, the Sixth Circuit upheld the adjustment where the defendant, after learning from a high school vocational program, built his own computer systems and modified consoles while trafficking in circumvention technology, noting that circuit precedent required self-taught skills to be "particularly sophisticated." United States v. Reichert, 747 F.3d 445, 454–55 (6th Cir. 2014) (quoting *Godman*, 223 F.3d at 323).

150 915 F.3d 1009, 1024–25 (5th Cir. 2019) (remanding for resentencing on §2D1.1(b)(12) (maintaining drug premises) and §3B1.3 issues). The Fifth Circuit also contrasted the defendant's knowledge and skills to the skills possessed by the defendant in *Reichert*, discussed above. *Id.*

151 "Bitcoin" is a form of digital cryptocurrency that is distributed on a peer-to-peer basis, where transactions are conducted directly between individuals with permanent, public records stored in a blockchain ledger. U.S. SENT'G COMM'N, PODCAST GLOSSARY ON EMERGING TECHNOLOGIES (2019), https://www.ussc.gov/sites/default/files/pdf/training/Podcasts/SPT_Emerging-Tech-Terms.pdf; *see also* United States v. Le, 902 F.3d 104, 108 n.3 (2d Cir. 2018) ("Bitcoin is a digital currency that is decentralized and pseudonymous, permitting online vendors and customers to maintain their anonymity by transferring the currency directly between their Bitcoin accounts, which contain no identifying information about either user.").

152 The "darknet" or "dark web" is part of the Internet that is not visible to regular search engines and may only be accessed through a special anonymizing browser (such as the "Tor" browser, which disguises internet activity by encrypting it). U.S. SENT'G COMM'N, SENTENCING PRACTICE TALK: THE DARK WEB (2019), https://www.ussc.gov/sentencing-practice-talk-episode-21-part-1. Defendants may commit crimes by computer through use of the dark web. *See*, *e.g.*, United States v. Ulbricht, 858 F.3d 71, 82 (2d Cir. 2017) (defendant operated an online marketplace on the dark web called the "Silk Road," which was "a massive, anonymous criminal marketplace that operated using the Tor Network[.]"); United States v. Schrank, 975 F.3d 534, 536 (6th Cir. 2020) ("Despite Schrank's alleged proficiency in computer systems, there is no 'ease of moving' through the dark web, as the district court suggests . . . . It takes a conscious effort, which includes downloading special software (normally Tor routing software) and using a specific sixteen-digit web address that is often obtained from other users . . . . This court is well-aware of the sophisticated operations of the dark web.") (internal citations omitted).

153 *Lord*, 915 F.3d at 1018.