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 To the extent this document includes unpublished cases, practitioners should be cognizant of Fed.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
- Robbery 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 1

II. COMPUTER ESPIONAGE 4

A. Relevant Statute: 18 U.S.C. § 1030(a)(1) (Computer Espionage) 4

B. Applicable Guideline: Section 2M3.2 (Gathering National Defense Information) 5

1. Base Offense Levels 5

2. Commentary 5

III. COMPUTER FRAUD 6

A. Relevant Statutes 6

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

2. 18 U.S.C. § 1037 (Fraud and Related Activity in Connection with Electronic Mail) 8

B. Applicable Guideline: Section 2B1.1 (Theft, Property Destruction, and Fraud) 9

1. Base Offense Levels 9

2. Specific Offense Characteristics 10

a. Loss 10

b. Mass marketing 12

c. Section 1037 offenses involving email addresses obtained through improper means 13

d. Sophisticated means 14

e. Device-making equipment and unauthorized access devices 15

f. Section 1030 offenses involving personal information and substantial disruption of critical infrastructures 17

g. Departures 18

IV. TRESPASSING ON A GOVERNMENT COMPUTER 20

A. Relevant Statute: 18 U.S.C. § 1030(a)(3) (Trespassing on a Government Computer) 20

B. Applicable Guideline: Section 2B2.3 (Trespass) 21

V. EXTORTION INVOLVING PROTECTED COMPUTERS 22

A. Relevant Statute: 18 U.S.C. § 1030(a)(7) (Extortion Involving Protected Computers) 22

B. Applicable Guideline: Section 2B3.2 (Extortion by Force or Threat of Injury or Serious Damage) 22

VI. CHAPTER THREE ADJUSTMENTS: SECTION 3B1.3 AND COMPUTERS 23

A. Abuse of Position of Trust 24

B. Use of Special Skill 26

I. INTRODUCTION TO COMPUTER CRIMES

This primer provides a general overview of the statutes, sentencing guidelines, and case law for federal 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 (Fraud and related activity in connection with computers) and 1037 (Fraud and related activity in connection with electronic mail), 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, which prohibits computer fraud and abuse. Section 1030(a) 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;[3]
>
> (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;[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)).

[2] *See* 18 U.S.C. §§ 1030, 1037. 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 SEXUAL ABUSE AND FAILURE TO REGISTER OFFENSES (2024), https://www.ussc.gov/guidelines/primers/sexual-abuse-and-failure-register-offenses.

[3] 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." *Id.* § 2332b(g)(5). Computer espionage under section 1030(a)(1) and its related guideline (§2M3.2) are discussed in detail below. *See infra* Section II.

[4] *Id.* § 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* Section III.

(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;[5]

(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;[6]

(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;[7]

(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;[8] and

(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.[9]

Through section 1030(b), the statute further prohibits attempt and conspiracy to commit the above offenses.[10]

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."[11] As such, cell phones and devices with data processors are "computers" within the meaning of the statute, as are cloud-based servers.[12] A "protected computer" is a computer:

---

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

6 *Id.* § 1030(a)(4).

7 *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." *Id.* § 2332b(g)(5).

8 *Id.* § 1030(a)(6).

9 *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* Section V.

10 *Id.* § 1030(b).

11 *Id.* § 1030(e)(1). The definition of "computer" expressly excludes automated typewriters, typesetters, portable hand-held calculators, and similar devices. *Id.*

12 *See, e.g.*, SkyHop Techs., Inc. v. Narra, 58 F.4th 1211, 1227 (11th Cir. 2023) (servers owned by Amazon Web Services, which are cloud-based, "clearly qualify as 'computer[s]' "); United States v. Streb, 36 F.4th 782,

> (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.[13]

Section 1030 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, cost incurred, or other consequential damages incurred because of interruption of service."[14] It defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[15]

In addition to other terms, the statute defines "exceeds authorized access" as "access[ing] a computer with authorization and us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[16] In *Van Buren v. United States*, the Supreme Court has held that a person "exceeds authorized access" in violation of section 1030(a)(2) when the person "accesses a computer with authorization but then obtains information located in particular areas of the computer—

791 (8th Cir. 2022) ("[A] cellphone is a 'computer,' at least under the 'broad' statutory definition" provided in 18 U.S.C. § 1030(e)(1) (citation omitted)); United States v. Mathis, 767 F.3d 1264, 1283 (11th Cir. 2014) (per curiam) (same), *abrogated on other grounds by* Lockhart v. United States, 577 U.S. 347 (2016); *see also* United States v. Wells, 29 F.4th 580, 588 (9th Cir. 2022) ("The definition of 'computer' under the condition [of supervised release] potentially could be understood to encompass common household objects[,] . . . such as smart kitchen appliances that contain microprocessors, even though such appliances are not capable of receiving, storing, or otherwise processing materials of child pornography.").

[13] 18 U.S.C. § 1030(e)(2).

[14] *Id.* § 1030(e)(11).

[15] *Id.* § 1030(e)(8).

[16] *Id.* § 1030(e)(6).

such as files, folders, or databases—that are off-limits to him."[17] However, the Court explained that section 1030 "does not cover those who . . . have improper motives for obtaining information that is otherwise available to them."[18] The Ninth Circuit has held that because the Supreme Court distinguished "between computer users who 'can or cannot access a computer system' " in *Van Buren*, the statute applies to only computers in which authorization is required and "does not apply to public websites."[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.

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]

---

17 593 U.S. 374, 396 (2021).

18 *Id.* at 378.

19 hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1198–99 (9th Cir. 2022) (quoting *Van Buren*, 593 U.S. at 390).

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

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

22 *Id.* § 1030(a)(1).

23 *Id.* § 1030(c)(1). 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 id.* § 2332b(g)(5)(A).

B. Applicable Guideline: Section 2M3.2 (Gathering National Defense Information)

Violations of 18 U.S.C. § 1030(a)(1) are referenced in Appendix A (Statutory Index) of the *Guidelines Manual* to §2M3.2, the guideline for offenses involving national security information.[24]

1. Base Offense Levels

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.

2. Commentary

The Commentary to §2M3.2 incorporates by reference the Commentary to §2M3.1 (Gathering or Transmitting National Defense Information to Aid a Foreign Government), including its definitions and departure considerations.[27] "Top secret information" is defined in §2M3.1 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

---

24 U.S. Sent'g Comm'n, Guidelines Manual App. A. (Nov. 2023) [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, 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.").

27 USSG §2M3.2, comment. (n.1).

28 USSG §2M3.1, comment. (n.1) (quoting Exec. Order No. 13526 (50 U.S.C. § 3161 note)).

29 USSG §2M3.1, comment. (n.2).

national security or further the nation's foreign policy objectives.[30] The Commentary further provides guidance on guideline application for convictions under other statutes.[31]

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 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.[32] Violations of subsection (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

[30] USSG §2M3.1, comment. (n.3).

[31] Application Note 2 to §2M3.2 instructs that, for convictions under 18 U.S.C. § 793(d) or (e) (Gathering, transmitting or losing defense information), 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 section 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 [the defendant] 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)").

[32] 18 U.S.C. § 1030(a)(2); *see*, *e.g.*, United States v. Agarwal, 24 F.4th 886, 888–89 (3d Cir. 2022) (contract network engineer retained access through credentials he was provided and unauthorized hardware and software enabling him to transfer information); 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). As noted above, the Supreme Court recently addressed the interpretation of "exceeds authorized access" and related statutory requirements in *Van Buren v. United States*, 593 U.S. 374 (2021). *See supra* notes 17–19 and accompanying text.

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.[33]

Subsection (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.[34] Violations of subsection (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.[35]

Section 1030(a)(5) prohibits knowingly causing the transmission of a program or code and intentionally or recklessly causing damage to a protected computer.[36] Penalties for a violation of subsection (a)(5) range from one year to life imprisonment.[37] 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.[38] 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.[39]

---

[33] 18 U.S.C. § 1030(c)(2).

[34] *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 [the defendant'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)").

[35] 18 U.S.C. § 1030(c)(3).

[36] *Id.* § 1030(a)(5); *see*, *e.g.*, United States v. Soybel, 13 F.4th 584, 594–95 (7th Cir. 2021) (defendant caused damage by issuing a change password command that temporarily prevented an authorized user from accessing a protected website, notwithstanding that other users were not affected and the issue was quickly resolved by the website operator); United States v. Gammell, 932 F.3d 1175, 1177–78 (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 subsection (a)(5)(A) that results in damage as defined in subsections 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).

[37] 18 U.S.C. § 1030(c)(4).

[38] *Id.* § 1030(c)(4)(A)(i)(VI).

[39] *Id.* § 1030(c)(4)(F).

Section 1030(a)(6) prohibits knowingly, and with intent to defraud, trafficking in passwords or similar access information.[40] Violations of subsection (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.[41]

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.[42] 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."[43] 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 three- or five-year statutory maximum term of imprisonment.[44]

[40] *Id.* § 1030(a)(6).

[41] *Id.* § 1030(c)(2)(A), (c)(2)(C).

[42] *Id.* § 1037(a)(1)–(5).

[43] *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).

[44] *See id.* § 1037(b). A violation of section 1037 carries 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 sections 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 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).

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.[45]

1. Base Offense Levels

Section 2B1.1(a) includes two alternative base offense levels. The higher of the two, base offense level 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."[46] If these conditions are not met, then the lower base offense level 6 applies.[47]

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,[48] 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.[49] "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.[50]

While many offenses involving computer fraud sentenced under §2B1.1 will likely start with a base offense level 6, some offenses may start with the alternative base offense

[45] *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 Offenses (2024), https://www.ussc.gov/guidelines/primers/intellectual-property.

[46] USSG §2B1.1(a)(1).

[47] USSG §2B1.1(a)(2).

[48] USSG §2B1.1, comment. (n.2(A)). For purposes of this base offense level, §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).").

[49] 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* USSG §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.").

[50] USSG §2B1.1, comment. (n.2(B)).

level 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 base offense level 7, because section 1030(c)(4)(E) (the relevant punishment provision) calls for a term of imprisonment of "not more than 20 years."[51] 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 base offense level 6 because its statutory maximum penalty is five years of imprisonment.[52]

2. Specific Offense Characteristics

Section 2B1.1 has 20 specific offense characteristics, some of which relate to conduct that occurs in computer crimes specifically. This section covers the specific offense characteristics 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.[53] The government must prove loss by a preponderance of the evidence.[54] The court need only make a reasonable estimate of the loss and is entitled to appropriate deference in its determination.[55]

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

51 *See* 18 U.S.C. § 1030(a)(5)(A), (c)(4)(E).

52 *See id.* § 1030(a)(2), (c)(2)(B).

53 *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.").

54 *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. Yihao Pu, 814 F.3d 818, 825 (7th Cir. 2016).

55 USSG §2B1.1, comment. (n.3(C)); *see also* 18 U.S.C. § 3742(e), (f). *See, e.g.*, United States v. Nicolescu, 17 F.4th 706, 721 (6th Cir. 2021) ("Although more specificity about [the loss] may have been preferable, 'the district court need only make a reasonable estimate of the loss using a preponderance of the evidence standard.' " (citations omitted)).

certain types of cases.[56] Application Note 3(A) instructs that "loss is the greater of actual loss or intended loss."[57] "Actual loss" is the reasonably foreseeable pecuniary harm resulting from the offense.[58] "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.[59] 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.[60]

---

[56] *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 (2024), https://www.ussc.gov/guidelines/primers/loss-calculation [hereinafter LOSS CALCULATIONS PRIMER].

[57] USSG §2B1.1, comment. (n.3(A)); *see also* United States v. Ayelotan, 917 F.3d 394, 408 (5th Cir. 2019) (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"). The Third Circuit has held, however, that loss means "actual loss" and declined to defer to the commentary. United States v. Banks, 55 F.4th 246, 255–58 (3d Cir. 2022).

[58] 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)).

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

[60] 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.").

"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.[61]

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.[62] 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.[63] Courts have interpreted loss in this context to include costs such as lost productivity, the cost of switching internet providers,[64] 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.[65]

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.[66]

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

[61] USSG §2B1.1, comment. (n.3(D)).

[62] 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.

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

[64] 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.

[65] 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).

[66] USSG §2B1.1, comment (n.3(F)(i)) ("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.").

computer fraud.[67] The Commentary to §2B1.1 defines "mass-marketing" as "a plan, 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."[68] The Commentary also instructs that this 2-level enhancement should be applied to any defendant convicted of section 1037 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).[69]

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.[70]

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

[67] USSG §2B1.1(b)(2) (stating to apply the greatest if the offense "(A)(i) involved 10 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"). 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 (2024), https://www.ussc.gov/guidelines/primers/economic-crime-victims.

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

[69] USSG §2B1.1, comment. (n.4(B)); *see also* USSG App. C, amend. 665 (effective Nov. 1, 2004) ("Because 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.").

[70] *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 into a fraud can vastly increase the scale of the fraud"); 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. 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 [the defendant] operated a website devoted to the solicitation of investments in his fraudulent scheme is sufficient" (citation omitted)); 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 [the defendant] posted an online advertisement that was open to the public shows that she designed her scheme to induce a large number of victims"). *But see* United States v. Bailey, 973 F.3d 548, 574 (6th Cir. 2020) (enhancement vacated where the defendant's only marketing was word-of-mouth marketing, which is already covered by statutes criminalizing fraud).

under 18 U.S.C. § 1037 and the offense involved obtaining email addresses through improper means.[71] Whereas application of most other specific offense characteristics 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.[72] 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.[73]

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.[74]

In addition, subsection (b)(10) establishes a minimum offense level of 12 in such cases.[75]

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 telemarketing scheme involving locations in multiple jurisdictions or hiding assets through fictitious entities, corporate shells, or offshore financial accounts.[76] 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

---

71 USSG §2B1.1(b)(6).

72 *Id.*; *see also* USSG §1B1.3, comment. (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.").

73 USSG §2B1.1, comment. (n.6). The Fifth Circuit upheld an enhancement under §2B1.1(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.*

74 USSG §2B1.1(b)(10).

75 *Id.*

76 USSG §2B1.1, comment. (n.9(B)).

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.[77]

Courts look at the totality of the circumstances surrounding the scheme to determine whether the offense involved sophisticated means.[78] Courts have upheld the sophisticated means enhancement in cases involving (1) manipulation of computer systems and financial records,[79] (2) manufacturing items by computer to make schemes appear legitimate,[80] (3) acquisition of personal information through email accounts,[81] and (4) repeated access to protected computers or systems to obtain usernames and passwords.[82]

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:

> (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

---

77 USSG §2B1.1, comment. (n.9(C)).

78 *See*, *e.g.*, United States v. Mitchell, 914 F.3d 581, 586 (8th Cir. 2019) ("Taken alone, the individual activities . . . were not extraordinarily intricate or high-tech—and sometimes were unsuccessful—but the scheme as a whole was sufficiently sophisticated."); 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.").

79 *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).

80 *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").

81 *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").

82 *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 the keyloggers [and] [t]he hacking involved multiple, repetitive and coordinated steps to deceive and exploit [the] protected system").

(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.[83]

Subsection (b)(11) also establishes a minimum offense level of 12.[84]

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."[85] 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."[86] Depending on the circumstances, the term "device-making equipment" may include keylogger software or computers equipped with digital templates for state identification cards.[87]

---

[83] USSG §2B1.1(b)(11). For defendants convicted of violating 18 U.S.C. § 1028A (Aggravated identity theft) 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 specific offense characteristic 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.*

[84] 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).").

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

[86] 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)).

[87] 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) ("[The defendant] possessed device-making equipment—his computer equipped with state identification templates—and he used that equipment to produce fake IDs for his writers." (footnote omitted)); *Barrington*, 648 F.3d at 1202 ("[T]he record evidence sufficiently supports a finding that 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

"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."[88] Social security numbers, usernames, and passwords may qualify as unauthorized access devices.[89]

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.[90] 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 specific offense characteristics in §2B1.1.

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."[91] Each subparagraph of the enhancement in §2B1.1(b)(18) targets different harms. 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.[92] 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.[93] 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

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" (citations omitted)).

88 USSG §2B1.1, comment. (n.10(A)); 18 U.S.C. § 1029(e)(3); *see also* 18 U.S.C. § 1029(e)(1) (defining "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)").

89 *See* United States v. Maitre, 898 F.3d 1151, 1160 (11th Cir. 2018) (driver's licenses, credit cards, debit cards, and social security numbers are "access devices"); 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 § 1029(e)(3)).

90 USSG §2B1.1(b)(18), (b)(19).

91 USSG §2B1.1(b)(18).

92 USSG §2B1.1(b)(18)(A).

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

medical records, private correspondence (including email), financial records, private photographs, or similar information.[94]

Second, like subsection (b)(18)(A), subsection (b)(19)(A) is offense-specific and requires a conviction under 18 U.S.C. § 1030.[95] 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."[96] "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."[97] A "critical infrastructure" may be publicly or privately owned and includes telecommunications networks, banking systems, emergency services, and transportation services.[98]

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."[99] In addition, an upward departure would be warranted if the 6-level increase at subsection (b)(19)(A)(iii) applies and the disruption "is so substantial as to have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters."[100]

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

94 USSG §2B1.1, comment. (n.1).

95 *See, e.g.*, United States v. Nicolescu, 17 F.4th 706, 730 (6th Cir. 2021) (district court erred in applying a 4-level enhancement under §2B1.1(b)(19)(A)(ii) because the defendants were not convicted of an offense under § 1030(a)(5)(A), but rather an alleged § 1030(a)(5)(A) violation as one of the objects of a conspiracy under 18 U.S.C. § 371).

96 USSG §2B1.1(b)(19)(A).

97 USSG §2B1.1, comment. (n.15(A)).

98 *Id.*

99 USSG §2B1.1(b)(19)(B); USSG §2B1.1, 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).

100 USSG §2B1.1, comment. (n.21(B)).

for offenses sentenced under §2B1.1 goes beyond monetary losses.[101] 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.[102]

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 substantially understates the seriousness of the offense.[103] 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,[104] including cases that involved "protected computers," access devices, and unlawfully obtained means of identification.[105]

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.[106] Under subparagraph (A)(v), courts may consider departing upward in cases involving stolen information from protected computers if the information

---

[101] *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 a protected computer "sought the 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.").

[102] 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 of the Primer 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 (2024), https://www.ussc.gov/guidelines/primers/departures-and-variances.

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

[104] 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)).

[105] USSG §2B1.1, comment. (n.21(A)(v)–(vi)). A "protected computer" is defined in section 1030(e)(2). *See supra* note 13 and accompanying text.

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

sought furthered a broader criminal purpose.[107] 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.[108]

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 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.[109]

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.[110] Such conduct is sometimes referred to as a computer "trespass."[111] 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.[112]

[107] 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).

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

[109] USSG §2B1.1, comment. (n.21(C)–(D)).

[110] 18 U.S.C. § 1030(a)(3).

[111] *See* USSG App. C, amend. 654 (effective Nov. 1, 2003).

[112] 18 U.S.C. § 1030(c)(2)(A), (c)(2)(C).

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

The applicable guideline for offenses under section 1030(a)(3) is §2B2.3 (Trespass).[113] Section 2B2.3 has a base offense level of 4, three specific offense characteristics, and one cross reference.[114] Two of the three offense characteristics directly involve computer crimes.[115] First, subsection (b)(1) provides for offense level increases if the trespass 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.[116] 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."[117]

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.[118] 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.[119] For purposes of §2B2.3, "protected computer" means a computer described in 18 U.S.C. § 1030(e)(2).[120]

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

---

113 USSG App. A.

114 USSG §2B2.3.

115 The specific offense characteristic that does not directly involve computers is the 2-level increase for possession of a dangerous weapon in §2B2.3(b)(2). *See* USSG §2B2.3(b)(2).

116 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).

117 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.* The definition of "critical infrastructure" at §2B2.3, comment. (n.1), is the same as at §2B1.1 and §2B3.2. *See* USSG §2B1.1, comment. (n.15(A)); USSG §2B3.2, comment. (n.1).

118 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.").

119 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 56.

120 USSG §2B2.3, comment. (n.1); *see supra* text accompanying note 13. The Commentary further incorporates the statutory definition of a "government entity" by reference to 18 U.S.C. § 1030(e)(9). *See* USSG §2B2.3, comment. (n.1).

determined under §2B2.3, the court applies §2X1.1 (Attempt, Solicitation, or Conspiracy).[121]

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.[122] 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.[123] 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.[124]

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.[125] Section 2B3.2 has a base offense level of 18, five specific offense characteristics, and two cross references.[126]

The specific offense characteristics in §2B3.2 provide offense level increases for a variety of aggravating circumstances, such as death threats, bodily injury, kidnapping, and loss.[127] Directly related to computers, subsection (b)(3)(B)(i)(V)[128] provides for a 3-level

---

121 USSG §2B2.3(c).

122 18 U.S.C. § 1030(a)(7).

123 *Id.* A "protected computer" is defined in section 1030(e)(2). *See supra* text accompanying note 13.

124 *Id.* § 1030(c)(3).

125 USSG App. A.

126 USSG §2B3.2. This section discusses one of the five specific offense characteristics 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).

127 USSG §2B3.2(b)(1), (b)(2), (b)(4), (b)(5).

128 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

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.[129]

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."[130] A "critical infrastructure" may be publicly or privately owned and includes telecommunications networks, banking systems, emergency services, and transportation services.[131] 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.[132]

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).[133]

---

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.").

129 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.

130 USSG §2B3.2, comment. (n.1).

131 *Id.* The definition of "critical infrastructure" at §2B3.2, comment. (n.1), is the same as at §2B1.1 and §2B2.3. *See* USSG §2B1.1, comment. (n.15(A)); USSG §2B2.3, comment. (n.1).

132 USSG §2B3.2, comment. (n.1); 18 U.S.C. § 1030(e)(9).

133 *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

Section 3B1.3 provides a 2-level adjustment in two circumstances: (1) if the defendant abused a position of trust; or (2) if the defendant used a special skill that significantly facilitated the commission or concealment of the offense,[134] both of which could apply to computer crimes. The government must prove the adjustment under either prong by a preponderance of the evidence.[135] The adjustment does not apply if an abuse of trust or special skill is included in the base offense level or specific offense characteristic.[136]

A. Abuse of Position of Trust

The first prong of §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.[137] "Public or private trust" refers to a position that is "characterized by professional or managerial discretion (*i.e.*, substantial discretionary judgment that is ordinarily given considerable deference)."[138] 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.[139] The adjustment applies even if the position of trust is fictitious.[140] In addition, the adjustment applies if the defendant abused his or her authority "to obtain, transfer, or issue unlawfully, or use without authority, any means of identification."[141]

---

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).

134 USSG §3B1.3.

135 *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).

136 USSG §3B1.3; *see*, *e.g.*, USSG §§2A3.3, 2C1.2, 2H1.1.

137 USSG §3B1.3.

138 USSG §3B1.3, comment. (n.1).

139 *Id.*

140 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, "[t]he 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").

141 USSG §3B1.3, comment. (n.2(B)); United States v. Cruz, 713 F.3d 600, 609 (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

The Commentary provides examples of appropriate application of the adjustment.[142]

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, decide whether the defendant used the position to significantly facilitate or conceal the offense.[143] Using this two-part test, the Fifth Circuit in *United States v. Miller* 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.[144] In contrast, the First Circuit in *United States v. Zehrung* vacated and remanded for supplemental findings the application of the abuse of trust adjustment in a federal healthcare-fraud case.[145] The

public or private trust," holding that Application Note 2's "own terms sever it from other §3B1.3 requirements . . . [so] Application Note 2(B) is an independent basis for applying an adjustment under §3B1.3").

[142] *See*, *e.g.*, USSG §3B1.3, comment. (n.1) (listing examples on the general applicability of the adjustment); USSG §3B1.3, comment. (n.2(B)) (listing examples involving means of identification); USSG §3B1.3, comment. (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).

[143] *See, e.g.*, United States v. Kowalski, 103 F.4th 1273, 1279 (7th Cir. 2024); United States v. Kingsbury, 107 F.4th 879, 881–82 (8th Cir. 2024); United States v. Douglas, 885 F.3d 124, 132 & n.2 (3d Cir. 2018) (en banc) (collecting cases). 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. Barringer, 25 F.4th 239, 254 (4th Cir. 2022); United States v. George, 841 F.3d 55, 67–69 (1st Cir. 2016); United States v. Alston, 899 F.3d 135, 151 (2d Cir. 2018) (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. Ghertler, 605 F.3d 1256, 1264 (11th Cir. 2010); United States v. Guidry, 199 F.3d 1150, 1160 (10th Cir. 1999). *But see* United States v. Moparty, 11 F.4th 280, 299 (5th Cir. 2021) ("The enhancement is appropriate if (1) 'the defendant occupies a position of trust' and (2) 'the defendant abused her position in a manner that significantly facilitated the commission or concealment of the offense.' " (citing United States v. Kay, 513 F.3d 432, 459 (5th Cir. 2007))); 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 "decisive factor" is the level of discretion given to an employee, and (2) the defendant abused the position of trust specifically with the victim of the offense charged. *See* United States v. Johnson, 79 F.4th 684, 713–14 (6th Cir. 2023) ("[First we] consider a defendant's 'level of discretion' as the 'decisive factor' " and "[s]econd, we consider a relationship with the victim." (citing United States v. Tribble, 206 F.3d 634, 637 (6th Cir. 2000))); 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."). 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).

[144] 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.

[145] 714 F.3d 628, 631–32 (1st Cir. 2013). 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.*, *Barringer*, 25 F.4th at 254; *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); *Ghertler*, 605 F.3d at 1264.

defendant used a computerized medical billing system to make false medical claims, but the sentencing court failed to show by a preponderance of the evidence that the defendant had the sufficient "professional or managerial discretion" required to be deemed to occupy a position of trust.[146]

B. USE OF SPECIAL SKILL

The second prong of section §3B1.3 provides for a 2-level adjustment if the defendant used a special skill that significantly facilitates the commission or concealment of the offense.[147] Unlike the first prong for abuse of trust, an adjustment solely for the use of a special skill may not be applied in addition to an adjustment under §3B1.1 (Aggravating Role).[148] The guidelines define a "special skill" as one "not possessed by members of the general public and usually requiring substantial education, training, or licensing."[149] The Sixth Circuit affirmed the adjustment where the defendant's self-taught technical expertise permitted him to defeat Digital Millennium Copyright Act circumvention technology because the skill could not be duplicated by persons of average ability.[150]

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

---

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. *Douglas*, 885 F.3d at 132–34. The court noted that its decision did not necessarily overrule its prior precedent relating to the adjustment. *See id.* at 133 n.5.

146 *Zehrung*, 714 F.3d at 630–33 (citing USSG §3B1.3, comment. (n.1)).

147 USSG §3B1.3.

148 *Id.*

149 USSG §3B1.3, comment. (n.4) (listing "pilots, lawyers, doctors, accountants, chemists, and demolition experts" as examples). The Fifth Circuit has held that self-taught computer "hacking" skills are not in the same class of "pilots, lawyers, doctors, accountants, chemists, and demolition experts." United States v. Lord, 915 F.3d 1009, 1022–25 (5th Cir. 2019) (citing United States v. Petersen, 98 F.3d 502, 507 (9th Cir. 1996)). 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) (holding "the word 'use' does not by its plain language include refraining from the use of one's skills," and adopting the approach of the Sixth Circuit, United States v. Weinstock, 153 F.3d 272 (6th Cir. 1998), which "differentiate[s] between [the defendant's] status . . . and using his skills," as opposed to the Third Circuit, 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' ").

150 United States v. Reichert, 747 F.3d 445, 454–55 (6th Cir. 2014) (upholding 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" (quoting United States v. Godman, 223 F.3d 320, 323 (6th Cir. 2000))); *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").

allowed him to access account numbers and withdraw money.[151] 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.[152]

In *United States v. Petersen*, 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.[153] First, the court upheld the district court's application of the adjustment based upon the defendant's "extraordinary knowledge" of computers.[154] 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."[155]

Other circuits have noted the above language in *Petersen* while analyzing, comparing, and contrasting courts' application of the "special skill" adjustment in cases involving computer crimes. For example, in *United States v. Lord*, involving failure to register a bitcoin[156] business and drug conspiracy, the Fifth Circuit followed the language in *Petersen* and reversed in part and remanded the defendant's case for resentencing because his self-taught computer "hacking" skills are not in the same class of "pilots, lawyers,

[151] 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").

[152] 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.").

[153] 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.

[154] *Id.* at 506–07.

[155] *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 *Petersen*. United States v. Lee, 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. *Id.* at 793–94. The Ninth Circuit reversed the district court's imposition of the special skills adjustment, citing the footnote in *Petersen*, because the defendant was "a video rental store operator who copied a web site . . . . [whose] level of sophistication was nothing like Petersen's." *Id.* at 799.

[156] "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.").

doctors, accountants, chemists, and demolition experts."[157] The Fifth Circuit explained that the 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[158] marketplace."[159]

[157] United States v. Lord, 915 F.3d 1009, 1022–25 (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.*

[158] 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). Sentencing Practice Talk*, The Dark Web*, U.S. SENT'G COMM'N, at 1:30 (Mar. 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."), *abrogated on other grounds by* Carpenter v. United States, 585 U.S. 296 (2018); United States v. Schrank, 975 F.3d 534, 536 (6th Cir. 2020) ("Despite [the defendant'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)).

[159] *Lord*, 915 F.3d at 1018, 1024–25.