



An Overview of Federal Criminal Laws Implicated by the COVID-19 Pandemic

April 13, 2020

As numerous [recent incidents](#) indicate, the ongoing coronavirus (COVID-19) pandemic’s impact [extends to the world of crime](#). News stories abound of attempts to profit from the pandemic by stockpiling [masks](#), [hand sanitizer](#), and [other staples](#) to sell at a [significant markup](#). Reports have also circulated about scams involving the sale of fake [COVID-19 test kits and cures](#), counterfeit [surgical masks](#), [substandard hand sanitizer](#), and [unauthorized medicines](#). Other fraudulent activities have not involved sales at all. [Some](#) have reportedly tried to use the pandemic to solicit donations to [illegitimate charities](#). In addition, the Federal Bureau of Investigation (FBI) has reported a spike in cyber-threats, including [COVID-19-related phishing emails](#)—messages designed to trick recipients into divulging personal information so the sender may access, for example, the recipient’s [email or bank accounts](#). Still other COVID-19-related illicit conduct is of a more violent nature, as evidenced by [recent reports](#) of individuals [publicly attacking](#) Asians and Asian Americans, erroneously accusing them of [causing or spreading COVID-19](#). The Department of Justice (DOJ) warns of the possibility of another offense: the intentional infection of or threat to infect others with COVID-19. These incidents and warnings suggest the possibility for COVID-19-related crimes, even as there is [some indication](#) that [crime rates](#) have [fallen](#) in some cities during the pandemic. Although [state criminal laws](#) likely govern much COVID-19-related conduct, given the [concern](#) expressed by [some Members](#) over the pandemic’s effect on justice and law enforcement issues, this Sidebar examines the primary federal criminal statutes that may be relevant to criminal activity related to the ongoing pandemic. It discusses, in order: (1) the [mail fraud](#) and [wire fraud](#) statutes, (2) the [Computer Fraud and Abuse Act \(CFAA\)](#), (3) the [Defense Production Act \(DPA\)](#), (4) [terrorism statutes](#) and [threat statutes](#), and (5) the [Matthew Shepard and James Byrd Jr. Hate Crimes Prevention Act \(HCPA\)](#).

Mail Fraud and Wire Fraud

Deceptive schemes to profit off of COVID-19, such as selling counterfeit medical supplies and sending phishing emails, could violate federal statutes prohibiting mail and wire fraud. The mail fraud statute, [18 U.S.C. § 1341](#), prohibits (1) [knowing or willing participation](#) in a scheme to defraud, (2) and use of the [United States Postal Service](#) or [commercial interstate carriers](#) (the mail) to further that scheme. Courts have interpreted “scheme to defraud” to [include](#) the “[common understanding](#)” of depriving someone of money or property by “dishonest methods” such as trickery and deceit. To violate § 1341, it need only be [reasonably foreseeable](#) that the mail would be used in furtherance of the scheme to defraud, which

Congressional Research Service

<https://crsreports.congress.gov>

LSB10446

requires only that the mail be “‘incident[al]’ to an essential part of the scheme” The elements of wire fraud under 18 U.S.C. § 1343 are [nearly identical](#) to those of mail fraud under § 1341, except § 1343 “[speaks of communications transmitted](#)” by [interstate wires](#), which may include, among other things, [emails](#), [telephone calls](#), [faxes](#), and [statements on websites](#). Although § 1343 specifically requires use of *interstate* wires, that requirement may be demonstrated with evidence of [transmission across state lines](#) or that an individual accessed “[information from \[an\] out-of-state computer](#).” Sections 1341 and 1343 criminalize a “[broad swath of behavior](#),” and their application to a given situation rests largely on prosecutorial discretion. Violations of [Sections 1341 and 1343](#) ordinarily may be punished by a maximum fine of [\\$250,000](#) or up to 20 years imprisonment, or both, but offenses that relate to a “presidentially declared major disaster or emergency” under the Stafford Act face [stiffer penalties](#) of up to \$1,000,000 fine, imprisonment for up to 30 years, or both. [Injunctions](#)—judicial orders requiring a person or entity to [cease an activity](#)—are also possible for violations of Sections 1341 and 1343.

A number of fraudulent activities reported in the context of COVID-19 might run afoul of Sections 1341 and 1343. Take, for example, the intentional sale of counterfeit surgical masks. The seller’s behavior—tricking the buyer into purchasing a product he believes has certain qualities that it actually lacks—would almost certainly be a scheme to defraud. If the seller used the mail in his scheme, such as to ship the masks, § 1341 would apply. If he relied on the internet, for example by soliciting buyers on a website, he most likely would have violated § 1343. Section 1343 may also prohibit, for example, [COVID-19-themed phishing emails](#), assuming that they involve schemes to defraud recipients of money or property, and were transmitted interstate. The DOJ has [successfully prosecuted](#) phishing scammers under §1343 in the past. Notably, not all applications of Sections 1341 and 1343 in the context of COVID-19 are [hypothetical](#). The DOJ has [already invoked § 1343](#) against a website purporting to offer vaccine kits, [which do not exist](#), in exchange for shipping fees, and against [a man](#) who allegedly solicited donations to fake charities. Those convicted of violating Sections 1341 and 1343 for actions related to COVID-19 may face enhanced penalties because President Trump has declared a national emergency [pursuant to the Stafford Act](#).

The Computer Fraud and Abuse Act

Some of the [reported COVID-19-related](#) schemes are uniquely computer based, including phishing schemes or attempts to install malware (i.e., unwanted software including [viruses and spyware](#)) on the computers of unsuspecting users. Such conduct could implicate the CFAA—an [anti-hacking law](#) covering most computers, including laptops, desktops, websites, and computerized devices. Several provisions of the CFAA focus specifically on “*protected computers*,” which [courts](#) have construed to include any computer connected to the internet. For example, the statute makes it a crime to “[knowingly cause\[\] the transmission](#) of a program, information, code, or command” and thereby “intentionally cause[] damage without authorization, to a protected computer.” The CFAA defines [damage](#) to mean “impairment to the integrity or availability of data, a program, a system, or information,” which [occurs](#), for example, where a hacker causes a computer to behave in a manner contrary to the intentions of its owner. The CFAA also contains antifraud provisions, such as one [subsection](#) that makes it a crime to “knowingly and with intent to defraud, access[] a protected computer without authorization, or exceed[] authorized access, and by means of such conduct further[] the intended fraud and” obtain something of value. The maximum penalties for [CFAA violations](#) vary based on the provision and gravity of the conduct.

Courts have applied the CFAA to [malware](#), and the DOJ has prosecuted [malware cases](#) and [phishing scammers](#) under the CFAA in the past. Some COVID-19-related malware schemes, such as one the FBI recently [described](#) as involving malware-infected emails purporting to be from the Centers for Disease Control and Prevention (CDC), may implicate the CFAA provision prohibiting damage to protected computers without authorization. The intent elements of that provision—knowing transmission and intent to damage—limit the statute’s reach, however. For example, it would not apply to someone who [recklessly or negligently](#) forwards a malware-infected, fake CDC-email. With respect to the prosecution of COVID-

19-related phishing attempts, the DOJ could rely on the CFAA’s antifraud provisions, assuming the phishing involves [intent](#) to defraud and obtains something of value—as in instances [where](#) the scammer uses personal information obtained through phishing to divert funds from the victim’s financial accounts.

The Defense Production Act

As noted, another crime related to the COVID-19 pandemic involves hoarding supplies to resell at a profit. Although such behavior may violate [state price-gouging laws](#), there [is no specific federal price gouging law](#) ([proposed legislation](#), discussed below, seeks to change that). However, a March 23, 2020 [Executive Order](#) (the Order) issued by President Trump prohibits some hoarding and price-gouging pursuant to the [DPA](#), which confers “upon the President a [broad set of authorities](#) to influence domestic industry” in the case of “national emergencies.” Among those powers, the President can designate “[scarce materials](#),” including “[any raw materials . . . commodities, articles, components . . . \[and\] products . . .](#)” Under 50 U.S.C. § 4512—aimed at “prevent[ing] hoarding”—it is illegal to accumulate materials that the President has designated as scarce “(1) [in excess of the reasonable demands of business, personal, or home consumption](#), or (2) for the purpose of resale at prices in excess of prevailing market prices” Willful violations [may be punished by](#) up to \$10,000 fine, one year of imprisonment, or both.

The [Order](#) invokes § 4512 and delegates to the Secretary of Health and Human Services (HHS) the President’s authority to designate scarce materials to combat COVID-19. In a notice effective March 25, 2020, the [HHS Secretary](#) designated a number of scarce materials, including certain respirators, ventilators, disinfecting products, surgical masks, and personal protective equipment. Attorney General Barr has clarified that the Order’s purpose is to prosecute “bad actors who amass critical supplies” for profiteering, not Americans [buying](#) necessities or “businesses acquiring materials needed for their own use.” The DOJ and HHS recently [confiscated](#) medical supplies from hoarders pursuant to the DPA. In addition, [some Members](#) have [introduced legislation](#) that would create a federal price-gouging law. For example, [one proposal](#) would prohibit the sale of goods or services during the COVID-19 emergency at “unconscionably excessive” prices and would task the Federal Trade Commission with enforcement. These proposals have tended to focus on enhancing civil penalties—for example, one [would impose](#) \$10,000 in civil penalties for price gouging—but at least one may also impose [criminal penalties](#).

Terrorism and Threat Statutes

As [two](#) recent [incidents](#) indicate, some individuals may intentionally spread COVID-19 or threaten to do so. Although those incidents resulted in [state prosecutions](#), such behavior may violate federal terrorism and threat statutes. For example, [18 U.S.C. § 175](#) imposes penalties of up to life imprisonment for anyone who “knowingly develops . . . transfers, acquires . . . or possesses any biological agent . . . for use as a weapon,” or threatens to do so. [Biological agents](#) include viruses “capable of causing . . . death” or disease in a human. Although § 175 only governs biological agents intended “for use as a weapon,” that term [excludes only](#) biological agents used for “prophylactic, protective, bona fide research, or other peaceful purposes.” Importantly, however, the Supreme Court has recognized that statutes like § 175 do not govern [local conduct](#) subject to state law, such as routine assaults involving biological agents. In determining whether conduct rises above the local level for the purpose of § 175, [courts](#) evaluate the dangerousness of the weapon and the harm that the weapon could cause. Another statute, [18 U.S.C. § 2332a](#), prohibits the actual, attempted, or threatened use of weapons of mass destruction against “any person or property within the United States,” when that action involves the mail, or interstate or foreign commerce. Weapons of mass destruction include biological agents, defined identically as in § 175. Violations of § 2332a may incur penalties of up to life in prison or capital punishment if death results from the offense. Sections 175 and 2332a both prohibit terroristic threats, and threats may also be punished under more general federal statutes, including [18 U.S.C. §§ 875](#) and [876](#). Both statutes impose a maximum penalty of five years imprisonment for threatening to injure someone, or twenty years if that

threat involves extortion. To violate § 875, the threat must be transmitted in “interstate or foreign commerce,” while to violate § 876, the threat must be sent through the mail.

In a [March 24, 2020 memorandum](#), the Deputy Attorney General suggested that the intentional spread, or threatened spread, of COVID-19, could be prosecuted under Sections 175, 875, 876, and 2332a. With respect to Sections 175 and 2332a, the coronavirus [appears](#) to be a biological agent because it is a [virus](#) that can cause disease or death. However, § 175 applies only to those who *knowingly* transfer a biological agent—so the statute would seemingly not apply to those who negligently or recklessly infect others with COVID-19. An additional limitation on the statute is whether the infection of others is wholly local conduct outside the scope of § 175. To decide, courts would likely examine the dangerousness of COVID-19 and the harm that could result from intentional infection. One question courts may face is whether the [contagiousness](#) of COVID-19 makes infecting a single person extra-local conduct because of the risk of subsequent spread. As for Sections 875, 876, and 2332a, they would only apply to the actual or threatened spread of COVID-19 if it involved the mail, or interstate or foreign commerce. That said, in specific circumstances, other statutes could also apply to the threatened infection of others, and the DOJ has filed such charges under statutes governing [biological weapons hoaxes](#) and [assault on federal officers](#).

The Hate Crimes Prevention Act

Some of the [reported](#) COVID-19-related attacks against Asians and Asian Americans might implicate the [HCPA](#). Under that statute, it is a crime to “willfully cause[] bodily injury to any person or, through the use of . . . a dangerous weapon” attempt to “cause bodily injury to any person because of the actual or perceived race, color, religion or national origin of any person.” Congress created that provision through its authority under the [Thirteenth Amendment](#) to prohibit “badges and incidents of slavery,” which includes “[most forms of racial discrimination](#)” and “[protects all races](#).” Thus, [courts](#) have applied the [protections of the HCPA](#) to crimes where the victims had various ethnic and racial backgrounds. The HCPA’s requirement that conduct occur “because of” race, color, religion, or national origin limits the statute’s otherwise broad scope. Courts have disagreed on the meaning of “because of.” At least one [court](#) requires that the conduct at issue would not have occurred *but for* the victim’s race, color, religion, or national origin. In contrast, other [courts](#) have interpreted “because of” more flexibly, requiring only that race, color, religion, or national origin be a “substantial motivating factor” in an attack, not the [only motivating factor](#). HCPA prosecution is [only possible](#) if the Attorney General or a designee certifies that (1) the state where the offense occurred lacks jurisdiction or requested federal prosecution; (2) state prosecution did not vindicate “the Federal interest in eradicating bias-motivated violence;” or (3) federal prosecution serves the public interest and is “necessary to secure substantial justice.”

As noted above, recent [news reports](#) have detailed COVID-19-related attacks on Asians and Asian Americans, such as one [widely-reported](#) attack on a Korean student in [Midtown Manhattan](#). The FBI has affirmed that “[investigating hate crimes remain\[s\] a high priority](#)” during the COVID-19 pandemic and is [reportedly](#) considering hate crimes charges against at least one suspect in this context. For the federal government to invoke the HCPA in the context of COVID-19-related hate crimes, the government would have to meet the HCPA’s certification requirements. The government would also have to establish that the victim’s perceived or actual identity as Asian or Asian American motivated the attack. As discussed above, the stringency of that requirement varies by jurisdiction. These offenses could be prosecuted under [state law](#), as [states](#) generally prosecute most hate crimes.

Author Information

Peter G. Berris
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.