COVID-19: Department of Justice Enforcement Against Scams

July 20, 2020

Congressional Research Service
https://crsreports.congress.gov
R46461

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46461

July 20, 2020

Kristin Finklea
Specialist in Domestic Security

COVID-19: Department of Justice Enforcement Against Scams

Criminals and other malicious actors often seek to capitalize on world events for their gain. Currently, some are leveraging the Coronavirus Disease 2019 (COVID-19) pandemic and relying on heightened public interest in it to take advantage of individuals and organizations. These schemes range from criminals claiming to be from a charitable organization or government agency and tricking individuals into providing money or personally identifiable information (PII) to fraudsters selling bogus or counterfeit treatments for COVID-19 or protective equipment and medical devices, that may or may not be delivered after victims submit payment. Further, scammers have tried to use stolen PII to gain access to and steal unemployment benefits and economic impact payments provided pursuant to the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; P.L. 116-136).

On March 16, 2020, Attorney General William Barr issued a memorandum to U.S. Attorney's Offices regarding the Department of Justice's (DOJ's) COVID-19 related enforcement priorities. The memorandum stated that "[e]very U.S. Attorney's Office is thus hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic." With the proliferation of COVID-19-related scams, federal law enforcement has established several specific mechanisms to coordinate efforts. For instance, the Attorney General requested that each U.S. Attorney's Office establish a Coronavirus Coordinator to serve as a legal counsel for the federal judicial district on COVID-19-related matters, prosecute or aid in the prosecution of COVID-19-related cases, and conduct public awareness and outreach activities regarding COVID-19 issues. Investigative agencies such as the Federal Bureau of Investigation (FBI) also lead and participate in task forces and working groups specifically targeting COVID-19-related scams.

DOJ has also conducted outreach to federal agencies charged with administering funding related to the CARES Act to help prevent and detect scams. In addition, DOJ has directed the public to report potential COVID-19 scams to the National Center for Disaster Fraud (NCDF), and the FBI points potential victims to several reporting systems, including the NCDF and the Internet Crime Complaint Center, and to reporting directly to the FBI through its tip line or local field offices.

In addition to establishing new efforts to counter COVID-19-related fraud, DOJ can leverage its existing tools to target scammers. Officials have noted that this fraud is often cyber enabled. Federal law enforcement has the principal role in investigating and attributing cyber incidents to specific perpetrators, and this responsibility has been established within the broader framework of federal cyber incident response. DOJ leads these efforts through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF). However, federal agencies involved in countering cyber threats and those related to COVID-19 are not limited to agencies within DOJ. Other federal law enforcement, such as the U.S. Secret Service, Immigration and Customs Enforcement's Homeland Security Investigations, and Customs and Border Protection have been working to investigate COVID-19 related scams, and entities such as the Federal Trade Commission, Cybersecurity and Infrastructure Security Agency, and the Department of the Treasury and the Department of Health and Human Services, among others, have been promoting public awareness about prominent scams.

Efforts from DOJ and other entities to counter COVID-19-related fraud involve both prevention (e.g., awareness campaigns) and response (e.g., investigations) activities. As policymakers examine the federal government's efforts to stop these scams, they may question the potential effects of agencies' investments in prevention activities and law enforcement response on reducing the prevalence and impacts of pandemic-related fraud. Relatedly, they may look to how the agencies themselves are evaluating the effects of the resources they have placed toward countering these scams.

Contents

Contacts

Criminals and other malicious actors often seek to capitalize on world events for their gain. Some criminals are leveraging heightened interest in the Coronavirus Disease 2019 (COVID-19) pandemic to take advantage of individuals and organizations.[1] Officials have cautioned about a host of scams and other criminal activity relating to the pandemic. These range from criminals claiming to be from a charitable organization or government agency and tricking individuals into providing money or personally identifiable information (PII) to fraudsters selling bogus or counterfeit treatments for COVID-19 or personal protective equipment (PPE) and medical devices that may or may not be delivered after victims submit payment.[2] The Federal Bureau of Investigation (FBI) noted that "as of May 28, 2020, the Internet Crime Complaint Center (IC3) received nearly the same amount of complaints in 2020 (about 320,000) as they had for the entirety of 2019 (about 400,000). Approximately 75% of these complaints are frauds and swindles."[3] In addition, the Federal Trade Commission (FTC) received more than 134,100 complaints (approximately 69,600 of which were specific to fraud) related to the COVID-19 pandemic, including the loss of over $87 million to fraud, in the first six and a half months of 2020.[4]

On March 16, 2020, Attorney General William Barr issued a memorandum to U.S. Attorney's Offices regarding the Department of Justice's (DOJ's) COVID-19-related enforcement priorities. The memorandum stated that "[e]very U.S. Attorney's Office is thus hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic."[5] Less than one week later, DOJ announced its first enforcement action against COVID-19 fraudsters. In doing so, the department alleged that the website "coronavirusmedicalkit.com" was claiming to provide consumers with access to World Health Organization (WHO) coronavirus vaccine kits if they provided their credit card information to pay for shipping.[6]

This report provides a brief overview of the types of scams criminals may use to steal money and PII from individuals and businesses. The report also discusses federal law enforcement's role—specifically, DOJ's role—in investigating and prosecuting these scams. Congress, in examining DOJ's priorities going forward, may look to the resources DOJ has placed toward countering fraud more broadly, and toward specific nefarious activity capitalizing on the COVID-19 pandemic.

[1] See, for example, Department of Justice (DOJ), *Combatting COVID-19 Fraud*, at https://www.justice.gov/coronavirus/combattingfraud. For more information on COVID-19, see the Centers for Disease Control and Prevention, *Coronavirus (COVID-19)*, at https://www.cdc.gov/coronavirus/2019-ncov/index.html.

[2] Federal Bureau of Investigation (FBI), Internet Crime Complaint Center, *FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic*, Alert Number I-032020-PSA, March 20, 2020.

[3] FBI testimony before the U.S. Congress, Senate Committee on the Judiciary, *COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic*, 116th Cong., 2nd sess., June 9, 2020.

[4] Federal Trade Commission (FTC), *FTC COVID-19 and Stimulus Reports, January 1, 2020 – July 16, 2020*, accessed July 19, 2020.

[5] Department of Justice (DOJ), *Memorandum for All United States Attorneys: COVID-19-Department of Justice Priorities*, March 16, 2020.

[6] Department of Justice (DOJ), "Federal Court Issues Temporary Restraining Order Against Website Offering Fraudulent Coronavirus Vaccine," press release, March 22, 2020. Notably, there are currently no approved vaccines to protect against COVID-19.

COVID-19 Scams

Generally, fraud is a profit-driven crime. Fraudsters may attempt to scam victims—individuals and organizations, including government programs—out of money directly or steal victims' personal information to profit in other ways. COVID-19-related fraud is no different.[7] While this section presents examples of COVID-19-related scams, it is not meant to be representative of the full spectrum of scams and tools criminals are utilizing to take advantage of the pandemic.

Scamming Victims Out of Money Directly

Fraudsters have used a number of scams to prey on public interest in the COVID-19 pandemic. People seek up-to-date information about the disease, attempt to purchase PPE such as masks, want to learn about or purchase preventive treatments or potential cures, and try to support front line workers and charities that deliver much-needed resources. The following are examples of how fraudsters take advantage of the pandemic.

- Swindlers have tried to sell counterfeit drugs and medical equipment or have pretended to sell PPE such as masks that are never delivered, scamming buyers out of money and potentially endangering lives. For example, DOJ arrested two individuals who tried to scam victims out of more than $4 million by falsely representing the legitimacy of their company and purporting to sell boxes of PPE; the boxes were empty, and law enforcement disrupted the scheme before victims lost their money.[8]
- DOJ filed a civil forfeiture complaint against several PayPal accounts associated with fraudulent websites. These websites were run by individuals in China purporting to sell masks; some victims never received anything, and others received alternate, nonmedical items such as toys or jewelry.[9]
- Law enforcement and consumer protection agencies have warned against scammers masquerading as charitable organizations addressing the pandemic.[10] The FBI has reported that "law enforcement has seen an increase in social media scams and telephone calls fraudulently seeking donations for illegitimate or non-existent charitable organizations requesting victims' bank account information."[11] The FBI has also worked with private sector internet domain providers and registrars to disrupt fraudsters, including taking down malicious websites such as one pretending to collect donations for American Red Cross COVID-19 relief efforts.[12]

[7] The Department of Justice is also countering price gouging and hoarding of goods related to the pandemic, but these are beyond the scope of this report.

[8] Department of Justice (DOJ), "Two Individuals Arrested for Conspiring to Defraud Purported Purchasers of Personal Protective Equipment," press release, April 27, 2020.

[9] Department of Justice (DOJ), "U.S. Files Civil Forfeiture Complaint in COVID-19 Fraud Case," press release, June 10, 2020.

[10] See, for example, Federal Trade Commission (FTC), *Make Your Coronavirus Donations Count*, May 5, 2020.

[11] Department of Justice (DOJ), *Coronavirus Response: Combatting COVID-19 Fraud*, at https://www.justice.gov/coronavirus/combattingfraud.

[12] Department of Justice (DOJ), "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams," press release, April 22, 2020.

Leveraging Stolen Personal Information

Criminals who steal victims' PII can use it to gain access to victims' existing accounts or establish new accounts that can be used for profit. For instance, scammers have tried to use stolen PII to redirect unemployment benefits and economic impact payments (EIP) provided pursuant to the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; P.L. 116-136). The Identity Theft Resource Center (ITRC) reports an uptick in queries related to COVID-19 fraud and that traffic to the center was 850% higher in March 2020 than in March 2019.[13] Fraudsters may use a number of tactics, including phone calls or email phishing[14] schemes in which they pretend to be a representative of a legitimate organization, to try and steal PII that they can then leverage to their advantage. The following are examples of how fraudsters have used interest in the pandemic to steal PII.

- Hackers have preyed upon public interest in mapping the spread of COVID-19. In one scheme, they sold a malware[15] infection kit to fraudsters who used an interactive map of COVID-19 cases produced by Johns Hopkins University to infect computers with malware. This malware was designed to steal passwords such that when unsuspecting users clicked on the map for information, their devices would become infected.[16] It is believed that hackers used the AZORult malware, "one of the most commonly bought and sold stealers in Russian [cybercrime] forums."[17]
- Thieves have used stolen PII to set up fraudulent accounts on the IRS website, and those who previously stole victims' PII and filed taxes using a stolen identity may also be able to receive the EIPs allocated to those individuals as part of the CARES Act.[18]
- DOJ has indicted individuals for attempting to defraud the government by filing false loan applications in attempts to receive forgivable Paycheck Protection Program (PPP) loans pursuant to the CARES Act. Some tried to swindle the government out of millions of dollars in loan money by falsifying business information.[19]

[13] Identity Theft Resource Center (ITRC), *COVID-19 Resources*, at https://www.idtheftcenter.org/covid-19-resources/. The ITRC is a nonprofit resource center focused primarily on supporting identity theft victims in the United States. See also Nathaniel Popper, "'Pure Hell for Victims' as Stimulus Programs Draw a Flood of Scammers," *The New York Times*, April 24, 2020.

[14] Phishing is "an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques." See U.S. Cybersecurity and Infrastructure Security Agency, at https://us-cert.cisa.gov/report-phishing.

[15] The term *malware* refers to "A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim." National Institute of Standards and Technology (NIST), "Malware," Computer Security Resources Center Glossary.

[16] "Live Coronavirus Map Used to Spread Malware," *Krebs On Security*, March 12, 2020.

[17] Alexander Eremin, Kaspersky, *AZORult++: Rewriting History*, March 22, 2019.

[18] Nathaniel Popper, "'Pure Hell for Victims' as Stimulus Programs Draw a Flood of Scammers," *The New York Times*, April 24, 2020. The IRS has issued warnings to taxpayers cautioning about potential fraud. See, for example, Internal Revenue Service (IRS), "IRS Issues Warning about Coronavirus-Related Scams; Watch Out for Schemes Tied to Economic Impact Payments," press release, April 2, 2020.

[19] See, for example, Department of Justice (DOJ), "Massachusetts Man Charged with COVID-Relief Fraud," press release, June 22, 2020.

- Fraudsters have taken advantage of the surge in unemployment claims and have used stolen PII to receive unemployment benefits. For example, the Secret Service issued an alert noting that a "well-organized Nigerian crime ring is exploiting the COVID-19 crisis by committing large-scale fraud against multiple state unemployment insurance programs, with potential losses in the hundreds of millions of dollars."[20] These criminals are reportedly using stolen PII to apply for state unemployment benefits and then relying on money mules, intermediaries often recruited through online romance scams, to receive the illicit money and forward it to them.[21]
- Law enforcement has received reports of scammers offering COVID-19 testing services in order to get Medicare beneficiary information, which they can then use to submit fraudulent medical claims for reimbursement—related or unrelated to COVID-19.[22]

While the pandemic may have presented new opportunities for criminals to leverage, fraudsters still rely upon a number of tried-and-true tools to scam victims or gain access to information, accounts, and resources. For instance, they continue to make robocalls, phish for information through emails and social media, install malware on unsuspecting users' devices, and exploit technology vulnerabilities. These scams generally seem to have a cyber component in that they are carried out or facilitated by the internet and evolving technology. In addition, criminals leverage both the surface web and dark web to facilitate these schemes.

Fraudsters on the Dark Web[23]

The layers of the internet go far beyond the surface content that many can easily access in their typical searches. The other content is that of the *deep web*, content that has not been indexed by traditional search engines such as Google. The furthest corners of the deep web, segments known as the *dark web*, contain content that has been *intentionally* concealed. The dark web may be used for legitimate purposes as well as to conceal criminal or otherwise malicious activities.

Fraudsters taking advantage of the COVID-19 pandemic have leveraged dark web marketplaces as an additional venue through which to sell legal or illegal, legitimate or counterfeit, and plentiful or scarce products and information. For instance, personal protective equipment such as N95 masks, gowns, and gloves have been found for sale on these marketplaces. In addition, there are reports that unapproved preventive drugs or cures such as the drug chloroquine[24] have been listed on these marketplaces. Even blood alleged to have belonged to recovered coronavirus patients was found for sale.[25]

However, it is unclear the extent to which scammers rely on the dark web instead of the surface web to sell pandemic-related goods and services and to carry out scams. For instance, the sale of some goods on the dark web may be limited by the "availability of similar goods on the surface web and the wider customer base not being traditional dark web users."[26] Reduced product supply on the surface web, though, could correlate with customers seeking these goods on the dark web.

[20] "U.S. Secret Service: 'Massive Fraud' Against State Unemployment Insurance Programs," *Krebs On Security*, May 16, 2020.

[21] Ibid. See also Mike Baker, "Feds Suspect Vast Fraud Network Is Targeting U.S. Unemployment Systems," *The New York Times*, May 17, 2020.

[22] Department of Justice (DOJ), *Department of Justice Enforcement Actions Related to COVID-19*, March 24, 2020.

[23] For more information on the dark web, see CRS Report R44101, *Dark Web*.

[24] For more information about chloroquine and related drugs, see CRS Insight IN11347, *Treatment of COVID-19: Hydroxychloroquine and Chloroquine*.

[25] Sooraj Shah, "Dark web scammers exploit Covid-19 fear and doubt," *BBC News*, May 19, 2020.

[26] EUROPOL, *Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic*, April 3, 2020, p. 10.

Department of Justice Response

With the proliferation of COVID-19 related scams, DOJ has established several specific mechanisms to coordinate efforts to combat them. For instance, DOJ has directed the public to report COVID-19-related scams to the National Center for Disaster Fraud (NCDF), within DOJ's Criminal Division. The NCDF's mission is to "improve and further the detection, prevention, investigation, and prosecution of fraud related to natural and man-made disasters, and to advocate for the victims of such fraud."[27] The FBI points potential victims to several reporting systems, including the NCDF and the Internet Crime Complaint Center (IC3), and to reporting directly to the bureau through its tip line or local FBI field offices.[28] Federal law enforcement therefore has a number of pathways to receive information about COVID-19-related scams. As Congress examines federal law enforcement's response to the pandemic, policymakers may look to these different pathways to see if they are sufficient to ensure that the full spectrum of reports are being received and that there are means to establish clear jurisdiction over particular crimes.

Reporting COVID-19 Scams

There is no central repository where individuals and organizations report complaints of fraud, COVID-19-related or otherwise. However, there are a number of reporting systems for the public to report suspected incidents of fraud, and those systems may share information to help law enforcement consolidate and deconflict public complaints about such incidents, including those related to COVID-19. Examples of federal entities to which victims may report include the following.

- **National Center for Disaster Fraud (NCDF).** The NCDF is a repository for the public to report complaints of disaster-related fraud to DOJ.[29] It was created in the wake of Hurricane Katrina and continues to serve as a resource for reporting fraud related to natural and man-made disasters.
- **Internet Crime Complaint Center (IC3).** The IC3 is a mechanism for the public to report all types of Internet-related crime to the FBI.[30] Originally established as the Internet Fraud Complaint Center in 2000, it was renamed in 2003 to reflect the nature of the internet- and cyber-related crimes reported to the center. In addition to providing information to law enforcement, the IC3 also shares alerts with industry partners and the public.
- **Consumer Sentinel.** The FTC's Consumer Sentinel is a mechanism for the public to report a range of consumer complaints to the commission, which in turn shares these complaints with law enforcement.[31] The Sentinel network provides law enforcement with tips on complaints, including frauds involving consumer product scams, credit and telemarketing scams, and identity theft.
- **FBI's tip line.** The FBI's system accepts tips on potential terrorist activity and reports of federal crimes such as fraud—including COVID-19-related fraud.[32] However, callers are directed to report internet-based fraud to the IC3. (In addition to the FBI, other federal, state, and local law enforcement entities have their own tip lines where individuals can report scams.[33])

[27] Ibid. See also Department of Justice (DOJ), *Department of Justice Coronavirus Response*, at https://www.justice.gov/coronavirus/DOJresponse. The NCDF, when appropriate, shares information with the FTC's Sentinel Database, which contains consumer complaints across a variety of categories (collecting complaints from at least 35 databases across the country) and is available to law enforcement.

[28] See https://www.fbi.gov/coronavirus.

[29] For more information, see https://www.justice.gov/disaster-fraud.

[30] For more information, see https://www.ic3.gov/about/default.aspx.

[31] For more information, see https://www.ftc.gov/enforcement/consumer-sentinel-network.

[32] For more information, see https://www.fbi.gov/tips.

[33] For example, U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) directs the public to report COVID-19 related fraud to a special DHS email tip line, COVID19FRAUD@DHS.gov, established for these types of reports.

In addition to providing mechanisms for the public to report information about COVID-19-related scams, DOJ has established several coordinated efforts to counter criminal activity associated with the pandemic. For example,

- the Attorney General requested that each U.S. Attorney's Office establish a Coronavirus Coordinator to serve as a legal counsel for the federal judicial district on COVID-19-related matters, prosecute or aid in the prosecution of COVID-19-related cases, and conduct public awareness and outreach activities regarding COVID-19[34];
- the FBI has formed—along with DOJ's Fraud Section and the Small Business Administration's Inspector General—a Paycheck Protection Program (PPP) Working Group to counter fraud against the program. The FBI reported that the working group had identified over $42 million in potential fraud and recovered over $900,000 as of early June 2020[35]; and
- DOJ's Criminal Division has "engaged in outreach to agencies tasked with implementing and overseeing CARES Act funds to design programs to detect and deter fraudulent conduct in the first instance. They are also coordinating with investigative agencies to identify key indicia of COVID-19/CARES Act related fraud schemes and to make sure information about emerging patterns and practices of fraudsters are shared across the relevant law enforcement community."[36]

In addition to establishing new efforts to counter COVID-19-related fraud, DOJ can leverage its existing tools to target scammers. As officials have noted, fraud related to COVID-19 is often cyber-enabled in some form[37]; the section below focuses on DOJ's role in countering cybercrime, including fraud.

DOJ's Role in Countering Cybercrime

Federal law enforcement has the principal role in investigating and attributing cyber incidents to specific perpetrators, and this responsibility has been established within the broader framework of federal cyber incident response. In a 2016 Presidential Policy Directive, the Obama Administration outlined how the government responds to *significant* cyber incidents—those that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[38] Responding to cyber incidents involves (1) threat response, (2) asset response, and (3) intelligence support. DOJ, through the FBI and National Cyber

[34] Department of Justice (DOJ), *Coordinated Nationwide Response to Detect, Deter, and Punish Crime Relating to the National Emergency Caused by COVID-19*, March 19, 2020.

[35] FBI testimony before the U.S. Congress, Senate Committee on the Judiciary, *COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic*, 116th Cong., 2nd sess., June 9, 2020.

[36] DOJ testimony before the U.S. Congress, Senate Committee on the Judiciary, *COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic*, 116th Cong., 2nd sess., June 9, 2020.

[37] See U.S. Secret Service testimony before the U.S. Congress, Senate Committee on the Judiciary, *COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic*, 116th Cong., 2nd sess., June 9, 2020.

[38] The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016. Of note, it is unclear whether any of the cyber incidents discussed in this CRS report may be considered a "significant cyber incident." Further, there have been no official indications that the Trump Administration has changed this approach to cyber incident response.

Investigative Joint Task Force (NCIJTF), is the designated lead on *threat response*.[39] Threat response involves

> conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.[40]

Defining a Cyber Incident

A principal issue in understanding how the federal government *responds* to a cyber incident is the definition of a *cyber incident*. A host of terms are used in discussing malicious activity with a cyber, online, or technological component. These range from cyber attack and cyberwarfare to cybercrime, cyber espionage, and cyber terrorism. A key distinction between these malicious incidents is the actor's motivation. For instance, a criminal may be profit motivated, while a terrorist may be politically motivated. However, "the speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all."[41]

Cyber incident, therefore, is an umbrella term encompassing a range of malicious activity carried out by diverse actors with varying motivations and capabilities—all of whom exploit cyberspace.[42] The federal government has defined a cyber incident as "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."[43]

As such, an incident could capture an array of activities carried out by malicious actors ranging from hacktivists and criminals to nation states and terrorists. Notably, the federal government has not developed official definitions for specific subsets of cyber incidents—such as cybercrime—that distinguish them from other subsets.[44]

FBI Cyber Investigations

The FBI pursues cybercrime cases ranging from computer hacking and intellectual property rights violations to child exploitation, fraud, and identity theft. Its top priorities involve combating

[39] For more information on the FBI's cyber investigations, see https://www.fbi.gov/investigate/cyber/. Information on the NCIJTF is available at https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. See also CRS Report R44926, *Justice Department's Role in Cyber Incident Response*. The Department of Homeland Security, through the National Cybersecurity and Communications Integration Center, is the lead on *asset response*. The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the lead on *intelligence support*.

[40] The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016.

[41] Department of Homeland Security (DHS), National Strategy to Secure Cyberspace, February 2003, p. viii.

[42] The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." In other words, cyberspace is the "virtual environment of information and interactions between people." National Security Agency, Statement for the Record, Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009.

[43] The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016. The PPD noted that this definition could include vulnerabilities in information systems, system security procedures, internal controls, or implementation that could ultimately be exploited by a threat actor.

[44] For a policy discussion on issues defining different types of cyber incidents (such as a definition of cybercrime), see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*.

computer and network intrusions and investigating ransomware. The FBI's cyber priorities focus on "high-level intrusions by state-sponsored hackers, global organized crime syndicates, and other technically sophisticated and dangerous actors."[45] It is unclear which portion of COVID-19 related scams might fall under these priorities.

The FBI leads a variety of law enforcement task forces and partnerships focused on cyber threat response.

- **National Cyber Investigative Joint Task Force (NCIJTF).** The NCIJTF was established by National Security Presidential Directive-54/Homeland Security Presidential Directive-23 in January 2008. As established, the NCIJTF's mission is to "serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations."[46] Led by the FBI, the NCIJTF coordinates over 20 U.S. agencies including law enforcement, intelligence, and the military. It also collaborates with the private sector and international partners.
- **Cyber Task Forces (CTFs).** There is a CTF at each FBI field office. These CTFs focus on local cybersecurity threats, respond to incidents, and maintain relationships with companies and institutions. They also support the national effort to combat cybercrime by participating in national virtual teams on certain cyber issues and providing cyber subject matter experts or surge capability outside of their field office jurisdiction, when needed.[47]
- **Cyber Action Teams (CATs).** In 2006, the FBI established CATs of agents and computer scientists that can be rapidly deployed around the country or the world to assist in computer-intrusion investigations. CAT members have expertise in various computer languages, forensic investigations, and analysis of malware.[48]
- **Cyber Assistant Legal Attachés (ALATs).** In addition to domestic field offices pursuing international leads in investigations, the FBI has positioned cyber ALATs in some foreign countries. These ALATs work with law enforcement in host countries to share information, collaborate on investigations, and enhance relationships with partner agencies. They focus on "identifying, disrupting, and dismantling cyber threat actors and organizations."[49]
- **Private Sector Partnerships.** In addition to the IC3, the FBI has established several initiatives to interface with the private sector and general public regarding cyber incidents. Through these initiatives, the FBI collects and shares information, builds partnerships, and enhances awareness. For instance, the National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit

[45] Statement of FBI Director Christopher Wray before the U.S. Congress, Senate Homeland Security and Governmental Affairs Committee, *Worldwide Threats*, 116th Cong., 1st sess., November 5, 2019.

[46] The White House, *National Security Presidential Directive-54/Homeland Security Presidential Directive-23*, January 8, 2008.

[47] Federal Bureau of Investigation (FBI), *Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity*.

[48] Federal Bureau of Investigation (FBI), *The Cyber Action Team: Rapidly Responding to Major Computer Intrusions*, March 4, 2015.

[49] Federal Bureau of Investigation (FBI), *National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly With Foreign Partners*, October 26, 2016. ALATs have been placed in London, England; The Hague, Netherlands; Tallinn, Estonia; Kyiv, Ukraine; and Ottawa, Canada, among other locations.

information-sharing organization that brings together subject matter experts from law enforcement, the private sector, and academia to target cybercrime; it produces unclassified intelligence assessments and develops strategies to mitigate cyber threats.[50] In addition, InfraGard is a collaboration between the FBI and private sector partners such as business executives, entrepreneurs, computer professionals, academia, the military, law enforcement, and other government officials; the program facilitates information sharing with the goal of protecting U.S. critical infrastructure.[51]

A Broad Federal Response

Federal agencies involved in countering COVID-19-related scams are not limited to those within DOJ. DOJ investigates and prosecutes fraud and provides consumer awareness, but federal efforts to counter these scams include agencies in other departments as well. For instance, within the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement Homeland Security Investigations (ICE HSI) launched Operation Stolen Promise to bring together the agency's "expertise in global trade investigations, financial fraud and cyber investigations with robust private and public partnerships to disrupt and dismantle this criminal activity [COVID-19 related fraud] and strengthen global supply-chain security."[52] In addition, ICE HSI works with U.S. Customs and Border Protection (CBP) to prevent smugglers from bringing "fraudulent, mislabeled, and unauthorized COVID-19 related products, such as purported anti-viral products, [PPE], and test kits" into the United States.[53] Further, the U.S. Secret Service and its electronic and financial crimes task forces investigate cyber-enabled financial crimes related to the pandemic. The Secret Service, like other federal law enforcement agencies, is also working on task forces specifically designed to counter pandemic-related fraud and conducting outreach with industry partners.[54]

In addition to investigating and prosecuting fraudsters exploiting the pandemic, federal agencies enhance public awareness of potential scams.[55] The Cybersecurity and Infrastructure Security Agency and FTC, for instance, provide tips to organizations and individuals on avoiding a range of pandemic-related scams. Other agencies provide awareness on industry-specific scams. For example, the Department of Health and Human Services provides awareness on testing, treatment, and Medicare-related scams; the Treasury Department's Inspector General warns about tax-related fraud; and the Social Security Administration warns about scams related to Social Security benefits.

Efforts from DOJ and other entities to counter COVID-19-related fraud involve both prevention (e.g., awareness campaigns) and response (e.g., investigations) activities. As policymakers examine the federal government's efforts to stop these scams, they may question the potential effects of agencies' investments in both prevention and response activities on reducing the

[50] For more information on the NCFTA, see https://www.ncfta.net/.

[51] For more information on InfraGard, see https://www.infragard.org.

[52] U.S. Immigration and Customs Enforcement (ICE), "ICE HSI launches Operation Stolen Promise," press release, April 15, 2020.

[53] U.S. Immigration and Customs Enforcement (ICE), "ICE HSI El Paso investigating COVID-19 related fraud, such as unauthorized test kits, face masks, diluted cleaning solutions, anti-viral products," press release, May 7, 2020.

[54] See U.S. Secret Service testimony before the U.S. Congress, Senate Committee on the Judiciary, *COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic*, 116th Cong., 2nd sess., June 9, 2020.

[55] For more information on agencies providing information about scams and fraud, see https://www.usa.gov/coronavirus.

prevalence and impacts of pandemic-related fraud. Relatedly, they may look to how the agencies themselves are evaluating the effects of the resources they have placed toward countering these scams.

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer