

COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic

Katelyn Wan Fei Ma¹ and Tammy McKinnon²

Abstract

The emergence of the novel coronavirus (COVID-19) has threatened physical and mental health, and changed the behaviour and decision-making processes of individuals, organisations, and institutions worldwide. As many services move online due to the pandemic, COVID-19-themed cyber fraud is also growing. This article explores cyber fraud victimization and cyber security threats during COVID-19 using psychological and traditional criminological theories. It also provides a COVID-19-themed cyber fraud taxonomy using empirical evidence from institutional and agency reports. Through organizing COVID-19-themed cyber fraud into four different categorizations, we aim to offer classification insights to researchers and industry professionals so that stakeholders can effectively manage emerging cyber fraud risks in our current pandemic.

Keywords

COVID-19; cyber fraud; cybercrime; cyber security; financial crime; infodemic; pandemic; policing; scams

Introduction

As of October 21st 2020, global COVID-19 cases have surpassed 40 million, while death tolls continue to rise and exceed the one million mark (World Health Organization, 2020). COVID-19 is an infectious disease caused by the SARS-COV2 virus, a coronavirus that primarily targets the human respiratory system (Rothan & Byrareddy, 2020). Infections with respiratory viruses are primarily transmitted through contact transmission, droplet transmission, and airborne transmission (Centers for Disease Control and Prevention, 2020). While some patients exhibit milder symptoms such as fever, cough, fatigue, headache, and diarrhoea, and are able to fully recover within weeks, others experience more severe symptoms including acute respiratory distress syndrome, acute cardiac injury, and incidence of grand-glass opacities that can lead to long-term damage and death (Rothan & Byrareddy, 2020). Because of the highly contagious nature of COVID-19, infection numbers continue to climb worldwide (Rothan & Byrareddy, 2020). On March 11th, the World Health Organization declared the COVID-19 outbreak a global pandemic, and many countries quickly responded to the declaration with strict social

¹ York University, Ontario, Canada

² Queen's University, Ontario, Canada

Corresponding Author:

Katelyn Wan Fei Ma, Department of Science & Technology Studies, York University, 218 Bethune College, 4700 Keele Street, Toronto, Ontario, Canada M3J 1P3
Email: katewm@yorku.ca

confinement enforcement (commonly referred as “lockdowns”) as an effective measure to manage human contact and virus transmission.

COVID-19 continues to impact our daily lives in various ways, and lockdown initiatives have reconfigured and reconstructed our social structures and environments. With stay at home orders, travel bans, and social distancing rules, internet use has spiked, as has reliance on online platforms including banking, healthcare, entertainment, business, education, and essential government services (Hakak, Khan, Imran, Choo & Shoaib, 2020). Many people have transitioned from working in an office setting to working from home; some are also taking part in a growing trend of online shopping, and individuals may choose to engage in virtual social events or dating instead of visiting friends or getting to know new people in the real world. Changes to consumer patterns and government responses have affected the ecosystems and economies of the cyber world. While consumers enjoy the convenience of online access and many online businesses and service providers have flourished in the context of COVID-19, not all online participants are legitimate. Specifically, cybercriminals now have more opportunities to exploit online service users in various creative ways. As the public moves from in-person to online activities, the likelihood of cybercrime victimization also increases, which may result in a disruption of services, financial loss, data breaches, and individual and institutional anxieties (Hakak et al., 2020).

This paper explores emerging cyber fraud threats during the pandemic by discussing some of the cyber fraud incidents we have observed in academic literature, law enforcement agency publications, and industry insight reports. Based on reported cyber fraud incidents, we hope to provide a COVID-19-themed cyber fraud pattern taxonomy using empirical evidence. For example, instead of discussing fraud techniques using a conceptual-to-empirical approach, we engage in an empirical-to-conceptual model and first identify a subset of categorization (Land, Smith, and Pang, 2013). We also hope to offer feasible and sustainable policy and regulation recommendations that can benefit a wider audience. As the COVID-19 outbreak has not been effectively contained worldwide at the time of writing (October 2020) and many countries are preparing for or already experiencing a second wave of infections (Strzelecki, 2020), our goal is to offer a COVID-19-themed cyber fraud trend observation and relevant viable global cyber security insights that can assist both industry professionals and the general public in curbing cyber fraud loss and cyber victimization.

Cyber Fraud Victimization: Exploring the Psychological Context

Before discussing the criminological perspectives, we believe it is crucial to explore the psychological context of cyber fraud victimization in our current climate. COVID-19 has not only changed people’s overall behaviour, but has also had significant impact on psychological and mental health. Many people have experienced emotional turbulence of various degrees during the pandemic, including but not limited to trauma and post-traumatic stress, depression, loneliness, generalized anxiety, insomnia, and suicidality (Lee, 2020). Understanding how people feel during a global pandemic helps researchers and industry professionals better comprehend individual decisions and choices.

Coronavirus anxiety may also induce physiological symptoms such as dizziness, sleep disturbance tonic immobility, appetite changes, and nausea or abdominal distress (Lee, 2020). Research results have shown that emotional distress is positively correlated with functional impairment, alcohol or drug abuse, negative religious coping, extreme hopelessness, and passive

suicidal ideation (Lee, 2020). In addition, people may also suffer from avoidance in meeting other people, while paradoxically also experience fear of social isolation (Kumar & Nayar, 2020). Furthermore, COVID-19-related social stigma has become another driving psychological factor that may impact behaviour and emotion. Kumar and Nayar's research suggests that many exposures to COVID-19 in India were due to international travel, but potential patients refused to get tested due to fears of social stigma and isolation (2020). What is making the situation worse is that, due to a lack of social and community support in many communities around the world, large populations suffer from additional anxiety due to loss of income and lack of access to basic essentials of life including food and shelter; this may lead to depression or even self-harm (Kumar & Nayar, 2020).

Cybercriminals target victims' psychological vulnerabilities, taking advantage of COVID-19-related anxiety by manipulating emotional instabilities to enable cyber fraud. Naidoo's research has shown that 30% of cyber fraud incidents involve cybercriminals targeting victims using relief as an emotional appeal, while 22% of cyber fraud events are associated with fear, and another 22% are associated with hope (2020). Other emotional appeals used in cyber fraud are enjoyment (15%), threat (6%), and compassion (5%) (Naidoo, 2020). For example, in order to utilize relief or hope as emotional elements to attract targeted victim's attention, cybercriminals may spread misinformation about possible cures / treatments or government relief funds; to facilitate fear or threat, cybercriminals may circulate COVID-19-related pressures, including local outbreaks, or use intimidating virus-related images to make victims feel vulnerable and concerned (Naidoo, 2020). Cybercriminals may also use enjoyment as an emotional appeal to encourage victims to purchase entertainment services, or to exploit people's compassion by soliciting donations to those in need (Naidoo, 2020). Research results show that cybercriminals tend to rely on sending positive emotional appeals to targeted victims to achieve monetary gains during this current pandemic.

Having explored the psychological context, it makes sense to speculate that many COVID-19-themed cyber fraud schemes are designed to target victims' stress, anxiety, and other emotional vulnerabilities. While we strongly believe that cybercriminals are capable of artistically designing different sophisticated fraud schemes catered to individual contexts, we believe it is essential to understand why cybercriminals do it and why they do it this way. The below section offers a theoretical analysis examining COVID-19-themed cyber fraud trends using classic criminological theories.

Understanding COVID-19-Themed Cyber Fraud with Traditional Criminological Theories

In this section, we would like to highlight two classic criminological theories that we find to be most applicable to COVID-19-related cyber fraud patterns: Anomie Theory and Strain Theory. In doing so, we attempt to understand the victimization and the causation of cyber fraud in a pandemic setting using criminological explanations. We hope that traditional criminological theories can provide academic insight to those who are interested in using classical theories to analyze new COVID-19-themed fraud trends today.

In Anomie Theory, Emile Durkheim (1893) argues that rapid social changes that occur in an organic society (in this case, the onset of COVID-19) will lead to the state of anomie. Anomie refers to a "breakdown of the ability of a society to regulate the natural drives of individuals in the face of rapid social change" (Cote, 2002, p. 96), which can lead to a state of normlessness.

Anomie Theory offers an explanation as to why some societies may have higher crime rates than others (Cote, 2002). A well-organized society with a highly specialized division of labour requires adequate regulations to maintain social order; if the regulation is inadequate, social problems such as criminal activities will more likely occur (Cote, 2002). In a rapidly changing society, when guidance and regulations are not provided to people in a timely manner, anomie may lead to confusion, insecurity, anxiety, and frustration, which would allow cybercriminals to exploit and abuse populations. When the COVID-19 outbreak began, most people were caught off guard and found themselves within a state of rapid societal change without always receiving clear or thorough instructions from leadership. New changes like working from home, using online services and online vendors, and becoming more socially active online all pose considerable cybersecurity challenges. From a victimization perspective, Anomie Theory offers insights into why people may be victimized by cyber fraud; from a perpetrator perspective, Anomie Theory provides an explanation as to why cyber fraud becomes an increasingly accessible criminal activity in our rapidly changing online environment.

Anomie Theory provides a viable explanation of cyber fraud victimization during COVID-19. In addition, Strain Theory can help explain the causation of such deviant cyber behaviours from within the pandemic setting. In a discussion of offenders' motivations and opportunities, Robert Merton (1957) continues to develop Durkheim's theory of anomie by arguing that stable social conditions may still allow the occurrence of criminal activities because of social structural strain (Cote, 2002). Merton indicates that each society has its own cultural and material goals "worth striving for," such as high personal value, high net worth, high degree of prestige, high social status, etc. (1957). In American culture, accumulated wealth is often associated with socially recognized success; in other words, one must have money to feel valued and respected (Cote, 2002). However, appropriate institutional structures or available legitimate channels of achieving such a goal is not always available to everyone, as many Americans are excluded from the social and financial networks that are necessary for success (Merton, 1957). Therefore, Merton developed Strain Theory, which suggests that the emphasis on achieving material gains outweighs the need to follow rules, which leads to individuals using any means necessary, including crime, to achieve such goals under social pressure (Choi, 2015). Looking through the lens of Strain Theory, we can see that cybercriminals may engage in criminal activities because of a perceived societal need to achieve monetary success. More specifically, in applying Strain Theory to the COVID-19 setting, we can see how perpetrators may engage in cyber fraud because of social strains and instabilities including job loss, insufficient food, and inadequate access to safe and secure shelter. Other motivations may include self-satisfaction, the need for peer respect, or even an attempt to impress potential employers in an organized crime ring setting (Wall, 2016). Strain Theory sheds light on the causation of cyber fraud during this time of acute and unique societal suffering.

Fraud Creativity: The Performative Nature of Cyber Fraud

After exploring the causation and the victimization of emerging cyber fraud trends from psychological and criminological perspectives, we can move on to discuss the various creative manifestations of cyber fraud today. There is no single way to conduct cyber fraud; a variety of deviant acts can be performed in the cyber world, as the online space allows for limitless creativity. Cybercriminals from all over the world have innovatively abused the cyberspace platform as a new stage to manipulate targeted victims, and victimization may be significantly

underreported (Wall, 2016). Victims may become involved in cyber fraud with or without the understanding of potential consequences; in some cases, victims may not acknowledge that they were involved in a cyber fraud incident or be reluctant to report such offences due to embarrassment and stigma. In instances such as money mule scams, where victims are manipulated by cybercriminals to move around illicit funds, victims may not even know that they have been involved in fraudulent activities, even if their financial activities clearly indicate that they have. According to Wall, when victimization is assessed using ideological, political, moral, or commercial evaluation, the victim may not be aware of, or may not believe, that they have been victimized (Wall, 2016). Wall suggests that hesitance to report may be tied to victims' embarrassment, ignorance of what to do or who to contact, or just simply "putting it down to experience" and wanting to move on with their lives (Wall, 2016).

Despite potential underreporting and the difficulties of drawing a precise boundary between regular cyber fraud and COVID-19-related cyber fraud, it is undeniable that COVID-19-related cyber fraud continues to grow alongside the spreading virus. Current academic research and industry reports have shown that fraudsters have put old wines into new bottles to defraud targeted victims by abusing the COVID-19 context. According to a report from the United States' Federal Trade Commission, as of October 21st 2020 the organization had received more than 223,000 COVID-19-related fraud or scam concerns, leading to over 160 million dollars of total fraud loss (Federal Trade Commission, 2020b). In Canada, over 5,200 COVID-19-related fraud reports have been submitted to the Canadian Anti-Fraud Centre, with reported losses of over 6.2 million dollars (Canadian Anti-Fraud Centre, 2020a). It is also important to note that the actual numbers may be much higher than what have been reported. Not all COVID-19-related fraud has been correctly file; some cases may be classified as regular fraud even if the crime is principally related to COVID-19. For example, an online investment scam may be reported as a regular fraud instead of a COVID-19-related fraud if the investment opportunity was not related to COVID-19. However, it is crucial to recognize that victims may be more vulnerable to these investment scams due to financial or psychological impacts of the pandemic. As highlighted earlier in the paper, cybercriminals target victims' psychological vulnerabilities, which may be more pronounced in the COVID-19 era, especially when emotional appeals like relief, hope, and fear are involved in the schemes (Naidoo, 2020). Upon understanding the possibility that the reported numbers for COVID-19-related fraud may not be comprehensive, we also think it is important to compare and contrast the regular fraud numbers pre and post COVID-19. The FTC Consumer Sentinel Network fraud trend report from the Federal Trade Commission shows a total of 848,403 fraud, identity theft, and other related cases were reported for Q1 2020. Comparatively, a total of 987,892 cases were reported for Q2 2020 and a total of 1,121,331 cases were reported for Q3 2020 (Federal Trade Commission, 2020c). While the numbers for Q4 are not yet published at the time of writing, it is easy to speculate that cases will continue to grow as pandemic continues.

To understand COVID-19-themed cyber fraud more systematically, we have built a taxonomy using an empirical-to-conceptual approach. By reviewing the outcome of an example of cyber fraud, we will be able to review cyber fraud characteristics from beginning to end. Currently, many works of literature in the field examine cyber fraud techniques (Abukari & Bankas, 2020; Bruno, 2020; Collier et al., 2020; Mohsin, 2020; Naidoo, 2020; Tran, 2020), but not many scholars have focused on end results as a classification approach. Inspired by Land, Smith, and Pang's classification methodology, we attempt here to use an empirical-to-conceptual approach to sort group characteristics into different dimensions (2013), and use deductive

reasoning to explore the trend and categories of cyber fraud. We would like to highlight that the examples categorized below may not be exclusive to each other, as some cyber fraud techniques overlap. However, such a taxonomy aims to guide the reader to understand the performative nature of cyber fraud, and how cyber fraud can be conducted creatively using various techniques. With this goal in mind, we have briefly broken down COVID-19-themed cyber fraud into the following categories:

- Unauthorized Transactions using Financial Information
- Unauthorized Transactions using Identity Information
- Authorized Transactions without Fraudulent Intent
- Authorized Transactions with Fraudulent Intent

Unauthorized Transactions using Financial Information

We define this category as events in which only financial information is compromised, meaning that while cyber fraud has occurred, the victim's personal identity is not jeopardized. This may be because fraudsters do not have the information needed to do so. Nevertheless, cybercriminals in this scenario do have enough financial information to achieve illegal monetary gains through unauthorized transactions. This can be achieved through stolen credit card information, either through compromised merchants or by using social engineering techniques to exploit victims' financial credentials. It can also be achieved through close relationship abuse such as elder abuse, in which a perpetrator manipulates a victim's trust or their personal relationship for financial gains.

One of the most common instances of cyber fraud is stolen credit card information, which can occur through compromised online merchants or the use of crimeware and social engineering techniques. While online merchants can themselves be fraudulent, this is not always the case. Chi Tran's research provides insight into domain spoofing, which is often associated with compromised merchants who may not know their domain has been spoofed. Five typical domain spoofing techniques include (1) top-level domain spoofing: who.int (legit) -> who(dot)edu (fake); (2) typosquatting: who.int (legit) -> whoo(dot)com (fake); (3) visual homograph: google.com (legit) -> g00g1e.com (fake); (4) semantic spoofing: who.int (legit) -> tedrosadhanom(dot)com (fake); 5) combination: who.int (legit) -> w^hoo(dot)edu (fake) (Tran, 2020). Spoofed domains become a viable and sustainable cyber fraud scheme platform for cybercriminals to obtain credit card information, especially when people experience COVID-19-related anxiety. Individuals may provide sensitive financial information to a fake website masked with spoofing techniques. In addition, cybercrime crimeware and social engineering also provide easy platforms for perpetrators to abuse. Gordon and Ford's research indicates that cybercrime crimeware includes, but is not limited to, trojans, viruses, bots (e.g. FriendBot), keyloggers, backdoors, e-skimming, spyware, ransomware, scareware, adware, worms, malicious code, and denial-of-service (2006, as cited in Naidoo, 2020). Other social engineering techniques include dumpster diving (physical and digital), surfing online content, reverse social engineering, role playing, shoulder surfing, and so on (Abukari & Bankas, 2020). All these techniques become means for cybercriminals to obtain sensitive financial information to conduct cyber fraud. With more people working from home and accessing services and products online, there are additional opportunities for cybercriminals to exercise their malicious techniques to their financial benefit (Tran, 2020).

Another type of unauthorized transactions that use victims' financial information involve elder abuse. While senior citizens are among those most severely impacted by COVID-19,

perpetrators have exploited the public health crisis by preying on the elderly through various fraud schemes (Department of Justice, 2020). Han and Mosqueda's research examines elder abuse in the COVID-19 era, looking at how older adults can be abused physically, emotionally, and / or financially (2020). Social distancing rules may help older populations avoid infection, but also increase older adults' multidimensional vulnerabilities, especially when "trusted others" such as family members, caregivers, neighbours, and friends are given access to sensitive financial information (Han & Mosqueda, 2020). Additionally, older adults may be less comfortable online, which necessitates handing over information to others to carry out basic tasks during the pandemic. When older adults have increased dependency on others during a lockdown setting, the potential for elder abuse is heightened; at the same time, the chances of perpetrators being caught has decreased (Han & Mosqueda, 2020; Makaroun, Bachrach & Rosland 2020). For example, caregivers may have access to victims' financial information for some legitimate purchases, but later conduct unauthorized transactions online without the victim's consent. When abuse occurs during lockdown, social support networks such as healthcare and crisis professionals, police, and Adults Protective Services may raise the bar for in-person evaluations, which makes elder abuse even harder to be identified or investigated (Makaroun et al., 2020).

Unauthorized Transactions using Identity Information

Unauthorized transactions using identity information represent an escalation from the previous categories of unauthorized transactions using financial information. In such classification, a victim's identity information is compromised, and the cybercriminal gains sufficient information to engage in cyber fraud. Cyber criminals take advantage of COVID-19 and profit from targeted victims' fears, uncertainties, and reliance on misinformation (Canadian Anti-Fraud Centre, 2020b). Common COVID-19-themed fraud schemes potentially compromising victims' identity information include government financial relief fraudulent application services and questionable contact tracer calls (Canadian Anti-Fraud Centre, 2020b; Federal Bureau of Investigation, 2020).

Countries such as the United States and Canada have introduced various financial relief programs like the Paycheck Protection Program (PPP) in the US and the Canada Emergency Response Benefit (CERB) and the Canada Emergency Student Benefit (CESB) in Canada. Cyber criminals can exploit these governmental relief programs through (1) offering help to qualified applicants in filling out financial relief program applications and consequently stealing victims' identities; (2) using victims' compromised identity information to file fraudulent financial relief program support, while the victim is either not qualified to receive such benefits or unaware of the application at all; or (3) impersonating government official to disqualify the benefit receiver and then contacting victims' for urgent repayment (Canadian Anti-Fraud Centre, 2020b; Federal Bureau of Investigation, 2020). Using fear and relief as emotional appeals, cybercriminals can easily tailor schemes to victims' vulnerabilities. As these fraud schemes often involve cyber criminals obtaining or requesting victims' identity information, fraudsters can then apply for government assistance, open financial institution accounts, and file various credit applications under victims' names online without proper authorization.

Another common COVID-19-related fraud involving identity compromise is contact tracer scamming (Federal Trade Commission, 2020a). Contact tracing occurs when health departments contact individuals to inform them that they may have been exposed to COVID-19. Unfortunately, fraudsters can pretend to be contact tracers, and may ask for targeted victims' bank account information or credit card numbers. Sometimes they may also ask for social

security / social insurance numbers for the purposes of identity theft, or ask for money transfers, gift cards, or cryptocurrency for immediate financial gain (Federal Trade Commission, 2020a). Some contact tracer scammers may even intimidate victims by threatening their immigration status or instruct them to download malware by clicking suspicious emails or text messages (Federal Trade Commission, 2020a). Similar to financial relief program fraud, contact tracer fraud also allows cybercriminals access to victims' identity information that can then be exploited.

Authorized Transactions without Fraudulent Intent

In this classification, victims tend to have authorized transactions that are fraudulent in nature but are conducted without victims having fraudulent intent or knowing that they are committing fraud. Examples include victims unknowingly depositing fraudulent or altered cheques, or receiving illicit or stolen money transfers without being aware that the source of the money is suspicious.

Romance fraud happens when individuals sincerely looking for romance online encounter fraudsters who abuse victims' trust by making fake profiles and building what may feel like a real, loving relationship (Action Fraud, 2020). Once the cyber criminal is confident that they have earned the victim's trust, they may ask the victim to help them through a difficult life situation by sending money (Action Fraud, 2020). In some cases, the cyber criminal may engage in a cheque-cashing scheme. The fraudster may pretend that they are living abroad and are unable to cash cheques. They will then send a large lump sum of money to the victim using fraudulent cheques that appear to be legitimate, then ask the victim to send a portion back to him/her overseas and keep the rest. In such situations, victims unknowingly commit a crime by cashing a fraudulent cheque (TransUnion, 2020). As COVID-19 lockdowns continue, cyber criminals can more easily exploit people's loneliness and need for attention and love for their own financial gain (BBC News, 2020).

Employment scams are also a common COVID-19-themed cyber fraud; in such cases, a fraudulent company quickly offers the victim a job without going through a formal hiring process. The perpetrator may make the victim pay an advance fee for "training" or make them buy expensive equipment and supplies to work from home. The victim may be "accidentally" overpaid through a fraudulent cheque and then will be asked to deposit the cheque to wire back the difference. Some victims may even be asked to purchase cryptocurrency as a part of their job using money that may be stolen (Better Business Bureau, 2020). As unemployment rates in many sectors spike during the pandemic, people are more vulnerable to online employment scams and can be easily manipulated and abused by cyber criminals.

Authorized Transactions with Fraudulent Intent

Fraudsters categorized under this classification are usually those with explicit fraudulent intent. Many people in this categorization intentionally engage in cybercrime for financial gain. They are often somewhat associated with organized crime rings and their fraudulent behaviours are acquired in organized crime group setting. Social learning theory explains how criminal values, ideas, techniques, and expressions are acquired through social learning processes, and rejects biological or pathological explanations of criminal behaviours (Choi, 2015). As COVID-19 and the rapid social changes it brings have made many suffer financial distress, some may be more susceptible to committing cyber fraud as per Strain Theory (Cote, 2002). For example, as COVID-19 escalates financial pressures, people may engage in fraudulent activities including

filing fraudulent credit card applications, misusing credit cards, issuing fraudulent cheques and abusing online cheque deposit functions, busting out credit cards or defaulting on loans (Levi, Bissell & Richardson, 1991; Naidoo, 2020). Some people may also engage in other cyber fraud activities for financial gain such as creating fake charities, or initiating fraudulent trading schemes, offering fake refunds, creating website domains, and so on (Naidoo, 2020).

According to the Federal Bureau of Investigation (FBI), virtual asset money laundering is another type of cyber fraud that has emerged. Fraudsters leverage fear and uncertainty and use victims' accounts to launder illicit funds online (2020). Cyber criminals utilize a complex virtual payment infrastructure and sophisticated fraud schemes to launder criminal proceeds, and as these transactions are not tied to any real-world identity, it can be hard for law enforcement to trace them (Federal Bureau of Investigation, 2020). Even though current published agency reports do not have a dedicated section reflecting COVID-19-related numbers, the Financial Action Task Force has observed an increased use of virtual assets to move and conceal illicit funds (Financial Action Task Force, 2020a). Virtual asset service providers from 19 different jurisdictions have reported over 134,500 suspicious transaction reports to regulatory bodies between 2018 and March of 2020 (Financial Action Task Force, 2020a). Based on the COVID-19-related virtual asset fraud schemes reported by FBI, we speculate the fraud incidents will continue to grow as pandemic continues. Currently identified virtual asset fraud schemes include, but are not limited to, blackmail attempts, work from home scams, paying for non-existent treatments/equipment, and investment scams (Federal Bureau of Investigation, 2020). Traditional financial gatekeepers for fraud, money laundering and terrorist financing may currently be pre-occupied with business continuity issues and therefore have a decreased capacity for monitoring the increase in suspicious transactions (Financial Action Task Force, 2020b).

Recommendations for the Emerging Threats

COVID-19 has accelerated our societal transformation into an online information economy. Manuel Castell identifies three distinct characteristics of an information economy: (1) informational productivity, implying the capacity for generating knowledge and processing or managing information; (2) global, referring to the economy, from financing to production, as organized on an international scale; (3) networked, signifying the internet being used to perform informational protocols that enable communication and the convergence of technologies (2020; as cited in Wall, 2016). COVID -19 has shaped our current information economy and will continue to reconfigure relationships between multiple players in cyberspace. As we continue to deploy social distancing rules and move our daily routines online to help manage the risks of COVID-19, the information economy will also adapt accordingly through modifying informational productivity and informational networks on a global scale. The emerging cyber fraud threats, therefore, are heightened in this pandemic setting. While the internet provides necessary connectivity and flexibility in this unprecedented global crisis, its inherent anonymity and cyber security risks also become social, and sometimes legal, concerns. The implications of cyber fraud and deviant online social behaviour challenge rules and regulations in the sphere of international jurisdiction law. Cyber fraud has emerged as a by-product of technological advancement, and has gradually shaped our global sociotechnical system in the context of the political economy. Emerging cyber fraud risks require urgent attention from various stakeholders both in the public and private sectors.

Though we fully acknowledge the countless challenges of staying cyber healthy during COVID-19, we would like to attempt to consolidate some recommendation for the general public, law enforcement and government agencies, and industry professionals. For the general public, we encourage the use of cyber security best practices including using trusted anti-virus software, checking web address details to avoid domain spoofing scams, and refraining from downloading attachments from suspicious emails or submitting sensitive financial information to untrusted websites. We also highly recommend potential victims to reconsider before taking action online, and to review one's emotional state carefully to examine if fraudsters may have used emotional appeals like relief, fear, hope, enjoyment, threat, or compassion, especially in these difficult times (Naidoo, 2020). Cyber fraud scams such as romance scams often leverage fake photos to attract victims' attention (TransUnion, 2020), therefore it is vital to learn the early warning signs such as perpetrators drawing on emotional attachments to fabricate a reason to ask for financial help (Action Fraud, 2020).

For law enforcement and government agencies, we encourage innovative thinking about designing policing regimes for cyber fraud, including private-public policing partnerships that leverage the private sector's efforts, and using decentralized networks in order to optimize the allocation of responsibilities, and making policing accountable to the public (Balkin, Grimmelmann, Eddan, Nimrod, Shlomit & Tal, 2007). Balkin et al. recommends improving policing accountability by building an optimal responsibility equilibrium, having liberal accountability values, and having a continuum of accountability (2007). There has been a chronic shortage of the law enforcement resources required to investigate and prosecute financial crime even before this current crisis. For instance, while there were 277,561 frauds reported to the police from 2017-2018 in the UK, only 8,313 cases resulted in a charge or summons, which is about 3% (The Police Foundation, 2018). This percentage fall significantly below the prosecution rates of many other crimes, such as violent offenses (15%), robberies (9%), theft (9%), sexual offences (6%), and all other police recorded offences (13.5%) (The Police Foundation, 2018). Furthermore, on average, cases related to fraud takes 514 days from reporting to charging, while theft offences take on about 50 days (The Police Foundation, 2018). The prolonged investigation time may disappoint victims, and consequently lead to victim disengagement and investigation ineffectiveness (The Police Foundation, 2018). Law enforcement and government agencies should allocate additional resources to handle complaints using a more holistic approach. Specifically, they should work with private sectors, including financial institutions and community support programs to fulfil minimum service levels so that victims' basic expectations can be met (The Police Foundation, 2018). While it is reasonable to allocate more investigation efforts to cases associated with higher dollar values, we believe it is also critical to perform primary investigation reviews and provide general guidance to victims associated with lower dollar value cases. This can include providing a platform for victims to track their cases through an online system and remain informed about the investigation progress (The Police Foundation, 2018). Such systems should be available to all actors, including victims, relevant law enforcement agencies, and victims' financial institutions so that all parties can work collectively to manage the risks of further fraud victimization.

To manage elder abuse, we recommend jurisdictions offer virtual "well calls" as an alternative to in-person home visits to reduce the risks of social isolation. Older populations can use such community support and resources to guard themselves against elder abuse and financial crime victimization (Payne, 2020). We also recommend the implementation of local victim support services that address the additional needs of more vulnerable population (The Police

Foundation, 2018). If elder abuse occurs, local victim support services should provide additional care and resources to more vulnerable victims who may lack autonomy to govern their own best interests. A standard governmental framework should be designed to identify, assess, and prioritize fraud related to vulnerability, and this framework criteria should be shared and practiced by all related actors.

For industry professionals in the fraud detection industry and cybersecurity industry, we recommend that the fraud detection industry develop more comprehensive detection systems to stop cyber fraud when it occurs on victims' accounts. This includes building a strong behavioural-based detection system, IP address-based detection systems, photograph-based detection systems, and text-based detection systems for applications (Huang, Stringhini & Yong, 2015). Researchers also recommend utilizing the integration of biometrics and Artificial Intelligence (AI) to improve authentication accuracy (Kairinos, 2019). Some practical examples of effective biometrics authentications are the Apple iPhone X Face ID system, which uses facial characteristics to unlock the device (with only about one per million error rate) and Samsung's development of iris scanning security, which recognises the unique patterns in a person's eye (Kairinos, 2019). While biometric techniques verify users' physical characteristics, AI can make the system even smarter by collecting and processing huge amounts of data at a rapid speed and constantly detecting threats when login or transactions patterns are disrupted (Kairinos, 2019). By actively engaging with AI-powered biometric security solutions, e-commerce and online banking sectors can continue to develop various strategies to detect and fight cyber fraud. Kairinos' research cites Mastercard as an example, a company that needs to monitor over 210 countries and territories and process over 165 million transactions every hour, Mastercard now uses a combination of machine learning algorithms and biometrics authentication information such as fingerprints and iris and facial recognition tools to help identify the identity of card users and mitigate potential fraud losses (2019). Machine learning also allows the ongoing learning of customers' behaviours based on past transactions and customer profiles. With pre-detection conditions filtered and biometrics information, financial institution can also strengthen their ability to detect elder abuse or impersonation fraud; for example, a sophisticated fraud detection system can more effectively alert the investigator when an elderly customer appears to apply online for a mortgage or a line of credit accompanied by suspicious login patterns or failed biometrics authentication. AI-driven biometrics security solutions can drastically increase the efficiency of the fraud detection industry and effectively allocate actors' investigation efforts.

Benefits of using AI-driven biometrics include but not limited to minimising the reliance on customers memorizing and retrieving passwords, removing human error from the process, and eliminating the possibilities of cybercriminals obtaining login credentials illegitimately (Kairinos, 2019). However, we also would like to highlight a few challenges associated with the pandemic situation. As wearing a mask is one of the most effective measures to prevent the spread of respiratory infections such as COVID-19, consumers are advised to wear face coverings when entering businesses or out in crowded public places (TechXplore, 2020). Consequently, it would become difficult to unlock a smartphone if the device uses facial characteristics as a security measure (TechXplore, 2020). Apple has released its iOS 13.5 iPhone software update to allow customers to directly enter a passcode to approve an Apple Pay transactions instead of waiting for several Face ID fails (TechXplore, 2020). Unfortunately, this takes away the security benefits of using device owner's biometrics and reverts the process back to passcode authentication. Similarly, for devices relying on fingerprints authentication, the authentication process may get jeopardized if the user wears disposable gloves and the process

will again revert to passcode authentication. We encourage industry professional to further explore AI-driven biometrics authentication methods that are compatible with personal protective equipment wearing practices.

For employees working from home, we recommend cyber security industry professionals harden employees' remote access by enforcing multi-factor authentication and virtual private networks (VPNs) to effectively manage the risk of phishing and shoulder surfing (Mohsin, 2020; Bruno, 2020). Additionally, instead of centralized encryption (which is a separated encryption process) we recommend that organizations use more secure end-to-end encryption (E2EE) that facilitates encrypted communication, so that classified data can be more safely guarded (Bruno, 2020).

In conclusion, this paper has presented a preliminary analysis of COVID-19-related cyber fraud trends and cyber fraud management opportunities. Upon examining current cyber fraud phenomenon using psychological research contexts and classical criminological theories, we then dissected the causation and victimization of COVID-19-related cyber fraud. We also explored the performativity of COVID-19-themed cyber fraud by conducting a taxonomy exercise, in which we broke down unauthorized transactions using financial information, unauthorized transactions using identity information, authorized transactions without fraudulent intent, and authorized transactions with fraudulent intent. Based on the empirical evidence and classification provided, we have tailored some recommendation for for the general public, law enforcement and government agencies, and industry professionals with the hope that all stakeholders can better manage the emerging cyber fraud risks in this difficult time.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

- Abukari, A. M., & Bankas, E. K. (2020). Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond. *International Journal of Scientific & Engineering Research*, 11(4), 7.
- Action Fraud. (2020). *Romance Fraud, Action Fraud*. <https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud>
- Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (2007). *Cybercrime: Digital Cops in a Networked Environment* (Vol. 4). NYU Press.
- BBC News. (2020). Coronavirus: Loneliness and Lockdown Exploited in Romance Scams. *British Broadcasting Corporation*. <https://www.bbc.com/news/business-52664539>
- Better Business Bureau. (2020). *BBB Tip: Employment Scams*. <https://www.bbb.org/article/tips/12261-bbb-tip-employment-scams>

Ma and McKinnon

- Bruno, D. (2020). *Covid-19 and Cybercrime: How Rogue Nations and Cyber Criminals Are Exploiting a Global Crisis*. Northern Policy Institute. <http://www.deslibris.ca/ID/10104022>
- Canadian Anti-Fraud Centre. (2020a). *Fraud Alert! COVID-19 fraud*. <https://www.antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm>
- Canadian Anti-Fraud Centre. (2020b). *The Impact of COVID-19 Fraud*. <https://www.antifraudcentre-centreantifraude.ca/index-eng.htm>
- Castells, M. (2010). *The Rise of the Network Society* (2nd ed., Vol. 1). Wiley-Blackwell.
- Centers for Disease Control and Prevention. (2020, February 11). *Coronavirus Disease 2019 (COVID-19)*. Centers for Disease Control and Prevention. <https://www.cdc.gov/coronavirus/2019-ncov/more/scientific-brief-sars-cov-2.html>
- Choi, K. (2015). *Cybercriminology and Digital Investigation*. LFB Scholarly Publishing.
- Collier, B., Horgan, S., Jones, R., & Shepherd, L. (2020). *The Implications of the COVID-19 Pandemic for Cybercrime Policing in Scotland: A Rapid Review of the Evidence and Future Considerations* (p. 19). Scottish Institute for Policing Research.
- Cote, S. (2002). *Criminological Theories: Bridging the Past to the Future*. Sage Publications.
- Department of Justice. (2020). *Department of Justice Observes 15th Annual World Elder Abuse Awareness Day*. <https://www.justice.gov/usao-or/pr/departement-justice-observe-15th-annual-world-elder-abuse-awareness-day>
- Durkheim, E. (1893). *The Division of Labor in Society*, translated by G. Simpson. Glencoe: Collier-Macmillan Ltd, 1964.
- Federal Bureau of Investigation. (2020). *COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic—FBI*. <https://www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic>
- Federal Trade Commission. (2020a). *Contact Tracing Call? 5 Things to Know*. 1.
- Federal Trade Commission. (2020b). *COVID-19 and Stimulus Reports*. <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map>
- Federal Trade Commission. (2020c). *Fraud & ID Theft Top Reports*. Tableau Software. https://public.tableau.com/views/TheBigViewAllSentinelReports/TrendsOverTime?%3Aembed=y&%3AshowVizHome=no&%3Adisplay_count=y&%3Adisplay_static_image=y&%3AbootstrapWhenNotified=true&%3Alanguage=en&.embed=y&.showVizHome=n&.apiID=host0#navType=0&navSrc=Parse
- Financial Action Task Force. (2020a). *12 Month Review of Revised FATF Standards—Virtual Assets and VASPs*.
- Financial Action Task Force. (2020b). *COVID-19-related Money Laundering and Terrorist Financing—Risks and Policy Responses*. 34.

- Hakak, S., Khan, W. Z., Imran, M., Choo, K.-K. R., & Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *IEEE Access*, 8, 124134–124144. <https://doi.org/10.1109/ACCESS.2020.3006172>
- Han, S. D., & Mosqueda, L. (2020). Elder Abuse in the COVID-19 Era. *Journal of the American Geriatrics Society*, 68(7), 1386–1387. <https://doi.org/10.1111/jgs.16496>
- Huang, J., Stringhini, G., & Yong, P. (2015). Quit Playing Games with My Heart: Understanding Online Dating Scams. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 216–236.
- Kairinos, N. (2019). The Integration of Biometrics and AI. *Biometric Technology Today*, 2019(5), 8–10. [https://doi.org/10.1016/S0969-4765\(19\)30069-4](https://doi.org/10.1016/S0969-4765(19)30069-4)
- Kumar, A., & Nayar, K. R. (2020). COVID 19 and its Mental Health Consequences. *Journal of Mental Health*, 1–2. <https://doi.org/10.1080/09638237.2020.1757052>
- Land, L., Smith, S., & Pang, V. (2013). Building a Taxonomy for Cybercrimes. *PACIS 2013 Proceedings*, 11.
- Lee, S. A. (2020). Coronavirus Anxiety Scale: A Brief Mental Health Screener for COVID-19 Related Anxiety. *Death Studies*, 44(7), 393–401. <https://doi.org/10.1080/07481187.2020.1748481>
- Levi, M., Bissell, P., & Richardson, T. (1991). *The Prevention of Cheque and Credit Card Fraud*. Home Office Crime Prevention Unit.
- Makaroun, L. K., Bachrach, R. L., & Rosland, A.-M. (2020). Elder Abuse in the Time of COVID-19—Increased Risks for Older Adults and Their Caregivers. *The American Journal of Geriatric Psychiatry*, 28(8), 876–880. <https://doi.org/10.1016/j.jagp.2020.05.017>
- Merton, R. K. (1957). Social Structure and Anomie. *American Sociological Review*, 3(5), 672–682.
- Mohsin, K. (2020). Cybersecurity in Corona Virus (COVID-19) Age. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3669810>
- Naidoo, R. (2020). A Multi-Level Influence Model of COVID-19 Themed Cybercrime. *European Journal of Information Systems*, 29(3), 306–321. <https://doi.org/10.1080/0960085X.2020.1771222>
- Payne, B. K. (2020). Criminals Work from Home during Pandemics Too: A Public Health Approach to Respond to Fraud and Crimes against those 50 and above. *American Journal of Criminal Justice*, 45(4), 563–577. <https://doi.org/10.1007/s12103-020-09532-6>
- Rothan, H. A., & Byrareddy, S. N. (2020). The Epidemiology and Pathogenesis of Coronavirus Disease (COVID-19) Outbreak. *Journal of Autoimmunity*, 109, 102433. <https://doi.org/10.1016/j.jaut.2020.102433>

- Strzelecki, A. (2020). The Second Worldwide Wave of Interest in Coronavirus Since the COVID-19 Outbreaks in South Korea, Italy and Iran: A Google Trends Study. *Brain, Behavior, and Immunity*, 88, 950–951. <https://doi.org/10.1016/j.bbi.2020.04.042>
- TechXplore. (2020, May 21). *Apple Face ID Fix: It Just Got a Little Easier to Unlock your iPhone while Wearing a Face Mask*. <https://techxplore.com/news/2020-05-apple-id-easier-iphone-mask.html>
- The Police Foundation. (2018). *More than Just a Number: Improving the Police Response to Victims of Fraud* (p. 102). https://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/more_than_just_a_number_exec_summary.pdf
- Tran, C. (2020). *Recommendations for Ordinary Users from Mitigating Phishing and Cybercrime Risks During COVID-19 Pandemic*. 7.
- TransUnion. (2020). *Dating Scams*. <https://www.iovation.com/topics/dating-scams>
- Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age* (Vol. 4). Polity.
- World Health Organization. (2020, October 21). *WHO Coronavirus Disease (COVID-19) Dashboard*. <https://covid19.who.int/>

Coronavirus-Related Fraud Prevention: Tips and Resources



The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) is a wide-ranging statute enacted on March 27, 2020, to address the health, economic, and societal impacts of the COVID-19 pandemic. At more than 300 pages, the Act is coupled with three other pieces of emergency legislation and provides \$2.4 trillion in economic relief to individual citizens, loans for businesses, support for hospitals and other medical providers, and economic relief for impacted businesses and industries. This legislation and other programs provide assistance to homeowners and renters, and to assist those in greatest need.

However, the trillions of dollars in economic relief appear to have incentivized those who seek to harm homeowners, mortgage borrowers, and renters through housing scams, loan modification and relief scams, and other forms of mortgage fraud.

Mortgage Borrowers and Renters

BE ON THE LOOKOUT FOR:

- ❖ Calls, emails, and text messages from individuals claiming to work for Fannie Mae or Freddie Mac, banks or mortgage companies, mortgage servicers, non-profits, or government officials, who offer lower interest rates, foreclosure relief, delayed payment terms, or other loan modifications. **If you receive a phone call that you think is suspicious, HANG UP! Should you choose to respond to such individuals, provide no personal information and do not offer to send money. Request the caller's name and contact information and report the call to us.**
- ❖ Unsolicited contact from individuals claiming to be affiliated with your bank, mortgage company, servicer, landlord, or management company. **If you receive a phone call that you think is suspicious, HANG UP! Should you choose to respond to such individuals, provide no personal information and request the individual's name and contact information and report the call to us.**
- ❖ Phone calls, emails, and text messages from individuals providing false information to make their communications appear to be legitimate. For example, your caller ID could show that the caller is your bank or Freddie Mac, but that may not be the case. **If you receive a phone call that you think is suspicious, HANG UP! Should you choose to respond to such**

If you think you have evidence of mortgage fraud, housing, or relief scams, contact our hotline at 1-800-793-7724 or file a complaint online at www.fhfa.org/ReportFraud#hotlineform

individuals, provide no personal information and request the individual's name and contact information and report the call to us.

- ❖ Offers for you to pay up-front by cash, check, or wire transfer for mortgage relief or rental assistance, that arrive by calls, emails, or text messages. **Because no legitimate relief program requires up-front payments, such offers are likely SCAMS. If you receive such an offer, do not respond, provide no information and provide no up-front money. Instead, ask for the offeror's name and contact information and report the offer to us. You can also report the scam to the Federal Trade Commission, at [FTC.GOV/COMPLAINT](https://www.ftc.gov/complaint).**
- ❖ Unsolicited contact from persons reporting to be affiliated with your bank or mortgage company, landlord, or management company. **Provide no information. Request the person's name and contact information, and verify whether the contact is legitimate by contacting your bank, mortgage company, landlord, or management company through a phone number on a recent bill or statement.**
- ❖ Unsolicited offers for mortgage or rental-related assistance. **Protect yourself and your family by insisting on obtaining and reviewing written materials explaining the proposed assistance, asking questions, and verifying whether the offer is legitimate.**
- ❖ Offers from individuals who seek to purchase your home and provide information about the consequences of loan forbearance. **Protect yourself and your family by insisting on obtaining and reviewing written materials explaining the proposed offer and consequences of loan forbearance, asking questions, and verifying the legitimacy of the information.**

REPORT SUSPECTED FRAUD, SCAMS, OR MISCONDUCT

Contact the [FHFA Office of Inspector General online](#) or call the hotline at 1-800-793-7724

OBTAIN MORE INFORMATION AND ASSISTANCE

You can find additional coronavirus-related fraud-prevention resources as well as mortgage help online and by telephone at:

- ❖ FHFA – [Mortgage Help for Homeowners Impacted by the Coronavirus](#)
- ❖ Consumer Financial Protection Bureau – [Guide to Coronavirus Mortgage Relief Options](#)
- ❖ Fannie Mae – [Beware of Scams](#) or 1-800-2FANNIE
- ❖ Freddie Mac – [Our COVID-19 Response](#) or 1-800-FREDDIE (select option 2)

If you have additional questions, contact your mortgage servicer (listed on a recent mortgage statement) for assistance.

Individuals Working in the Mortgage Industry

BE ON THE LOOKOUT FOR:

- ❖ Appraisal fraud by individuals misusing flexible appraisal alternatives;
- ❖ Application fraud by individuals exploiting borrower employment verification flexibility;
- ❖ Forbearance and foreclosure-rescue related fraud;
- ❖ Fraud related to property inspection and maintenance for delinquent properties; and
- ❖ Possible misappropriation of escrow funds.

REPORT SUSPECTED FRAUD, SCAMS, OR MISCONDUCT

Contact the [FHFA Office of Inspector General online](#) or call the hotline at 1-800-793-7724 in addition to statutory and regulatory reporting requirements

OBTAIN MORE INFORMATION AND ASSISTANCE

The Financial Crimes Enforcement Network (FinCEN) has issued information for financial institutions about COVID-19:

- ❖ [FinCEN Encourages Financial Institutions to Communicate Concerns Related to the Coronavirus Disease 2019 \(COVID-19\) and to Remain Alert to Related Illicit Financial Activity](#); and
- ❖ [FinCEN Provides Further Information to Financial Institutions in Response to the Coronavirus Disease 2019 \(COVID-19\) Pandemic](#)

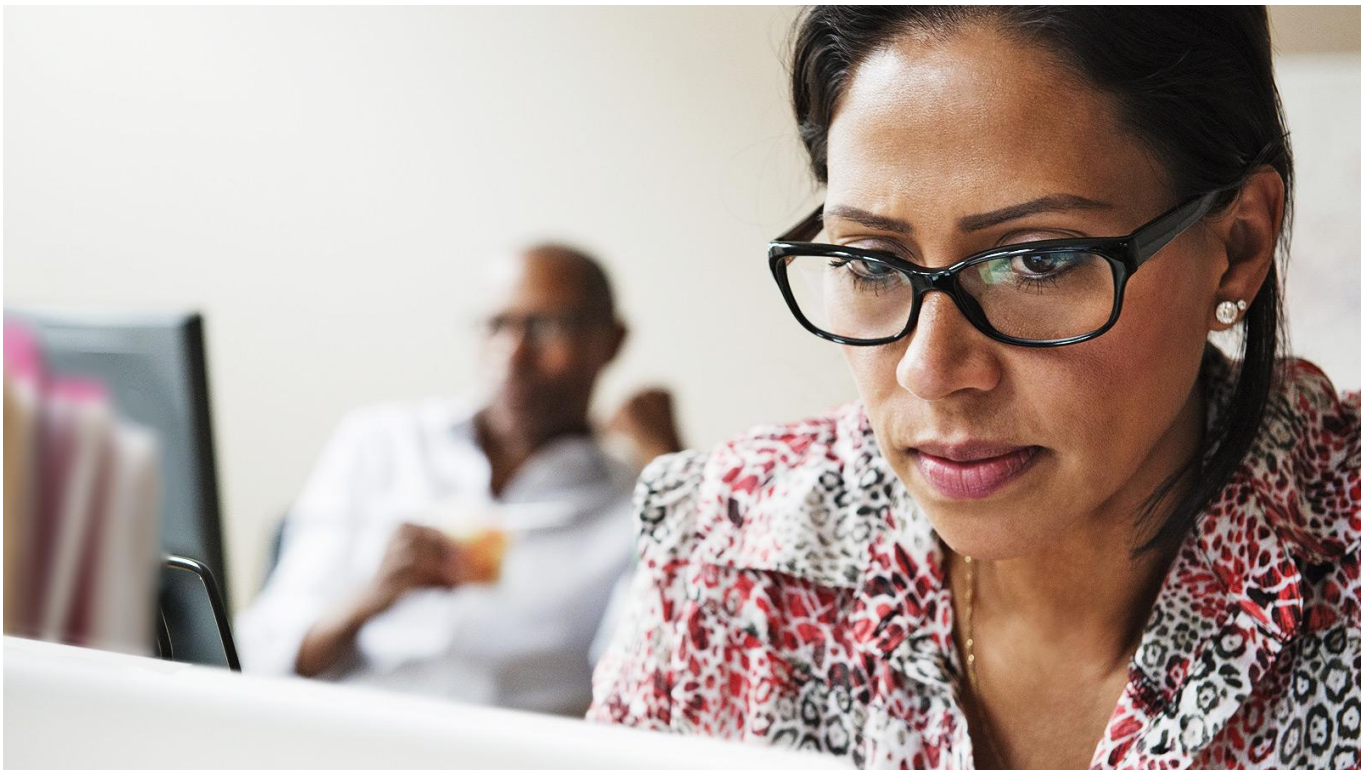
Fannie Mae and Freddie Mac have posted additional fraud-prevention resources for individuals in the mortgage industry that are available online from:

- ❖ [Fannie Mae – Mortgage Fraud Prevention](#)
- ❖ [Freddie Mac – Client Resource Center](#)

COVID-19 Frequently Asked Questions

On this page:

- General Information
- Vaccines, Biologics, Human Tissues, and Blood Products
- Drugs (Medicines)
- Medical Devices Including Tests for COVID-19
- Food Products
- Animals, Pets and Animal Drug Products



[Español \(/about-fda/fda-en-espanol/preguntas-frecuentes-sobre-la-enfermedad-del-coronavirus-2019-covid-19\)](#)

Along with other federal, state, and local agencies and public health officials across the country, the FDA continues critical work to protect public health during the COVID-19 pandemic. Find the most recent FDA updates on our Coronavirus Disease 2019 ([/emergency-preparedness-and-response/counterterrorism-and-emerging-threats/coronavirus-disease-2019-covid-19](#)) page.

The Centers for Disease Control and Prevention (CDC) has basic information about COVID-19 on their website at www.cdc.gov/coronavirus ([//www.cdc.gov/coronavirus](http://www.cdc.gov/coronavirus)).

The frequently asked questions (FAQs) on this page are for a general public or consumer audience. Other audiences may want to refer to additional FAQs:

- [Hand sanitizers and COVID-19 FAQs \(/drugs/information-drug-class/qa-consumers-hand-sanitizers-and-covid-19\)](/drugs/information-drug-class/qa-consumers-hand-sanitizers-and-covid-19)
- [Testing for SARS-CoV-2 FAQs \(/medical-devices/coronavirus-covid-19-and-medical-devices/faqs-testing-sars-cov-2\)](/medical-devices/coronavirus-covid-19-and-medical-devices/faqs-testing-sars-cov-2)
- [Medical glove FAQs \(/medical-devices/coronavirus-covid-19-and-medical-devices/medical-gloves-covid-19\)](/medical-devices/coronavirus-covid-19-and-medical-devices/medical-gloves-covid-19)
- [Surgical mask and gown shortage FAQs \(/medical-devices/personal-protective-equipment-infection-control/faqs-shortages-surgical-masks-and-gowns-during-covid-19-pandemic\)](/medical-devices/personal-protective-equipment-infection-control/faqs-shortages-surgical-masks-and-gowns-during-covid-19-pandemic)
- [3D Printing of Medical Devices & Parts FAQs \(/medical-devices/coronavirus-covid-19-and-medical-devices/3d-printing-medical-devices-accessories-components-and-parts-during-covid-19-pandemic\)](/medical-devices/coronavirus-covid-19-and-medical-devices/3d-printing-medical-devices-accessories-components-and-parts-during-covid-19-pandemic)
- [FAQs on Ventilators \(/medical-devices/coronavirus-covid-19-and-medical-devices/ventilators-and-ventilator-accessories-covid-19\)](/medical-devices/coronavirus-covid-19-and-medical-devices/ventilators-and-ventilator-accessories-covid-19)
- [Manufacturing, Supply Chain, and Drug Inspections FAQs \(/drugs/coronavirus-covid-19-drugs/manufacturing-supply-chain-and-drug-inspections-covid-19\)](/drugs/coronavirus-covid-19-drugs/manufacturing-supply-chain-and-drug-inspections-covid-19)
- [Food Safety and COVID-19 FAQs for Industry \(/food/food-safety-during-emergencies/food-safety-and-coronavirus-disease-2019-covid-19\)](/food/food-safety-during-emergencies/food-safety-and-coronavirus-disease-2019-covid-19)
- [Animal Food Safety and COVID-19 Industry FAQs \(/animal-veterinary/animal-health-safety-and-coronavirus-disease-2019-covid-19/industry-faqs-animal-food-safety-and-coronavirus-disease-2019-covid-19\)](/animal-veterinary/animal-health-safety-and-coronavirus-disease-2019-covid-19/industry-faqs-animal-food-safety-and-coronavirus-disease-2019-covid-19)
- [Face Mask and Surgical Mask FAQs \(/medical-devices/coronavirus-covid-19-and-medical-devices/face-masks-including-surgical-masks-and-respirators-covid-19\)](/medical-devices/coronavirus-covid-19-and-medical-devices/face-masks-including-surgical-masks-and-respirators-covid-19)

General Information

Q: What is the FDA doing to respond to the COVID-19 pandemic?

A: The FDA, along with other federal, state, and local agencies and public health officials across the country and internationally, plays a critical role in protecting public health during the COVID-19 pandemic. FDA staff are working around the clock to support


development of medical countermeasures (/emergency-preparedness-and-response/about-mcmi/what-are-medical-countermeasures) and are providing regulatory advice, guidance, and technical assistance to advance the development and availability of vaccines, therapies, diagnostic tests and other medical devices for use diagnosing, treating, and preventing this novel virus. The FDA continues to monitor the human and animal food supply and take swift action on fraudulent COVID-19 products.

Q: What is an emergency use authorization and how is it being used to respond to COVID-19?

A: In certain types of emergencies, the FDA can issue an emergency use authorization, or EUA, to provide more timely access to critical medical products (including medicines and tests) that may help during the emergency when there are no adequate, approved, and available alternative options.

The EUA process is different than FDA approval, clearance, or licensing because the EUA standard may permit authorization based on significantly less data than would be required for approval, clearance, or licensing by the FDA. This enables the FDA to authorize the emergency use of medical products that meet the criteria within weeks rather than months to years.

EUAs are in effect until the emergency declaration ends but can be revised or revoked as we evaluate the needs during the emergency and new data on the product's safety and effectiveness, or as products meet the criteria to become approved, cleared, or licensed by the FDA.

- Learn more about EUAs in this video (<https://youtu.be/iGkwaESsGBQ>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)
- Read more about COVID-19 tests (/consumers/consumer-updates/coronavirus-disease-2019-testing-basics)
- Find a community-based testing site (<https://www.hhs.gov/coronavirus/community-based-testing-sites/index.html>)

Q: How can I prevent COVID-19?

A: The best way to prevent illness is to avoid being exposed to the virus. The CDC recommends everyday preventive actions to help prevent the spread of respiratory diseases. They include:

- **Wash your hands** often with plain soap and water. The CDC recommends washing your hands often with soap and water for at least 20 seconds, especially after you have been in a public place, or after blowing your nose, coughing, or sneezing. If soap and water are not available, the CDC recommends using an alcohol-based hand sanitizer that contains at least 60 percent alcohol. Learn more about safely using hand sanitizer (</consumers/consumer-updates/safely-using-hand-sanitizer>).
- **Cover your mouth and nose** with a cloth face covering or non-surgical mask (<https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/cloth-face-cover-guidance.html>) when around others. Find more information about how to select, wear, and clean your mask (<https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/about-face-coverings.html>).
- **Avoid crowds and practice social distancing** (stay at least 6 feet apart from others).

Learn how to protect your family in this Consumer Update (</consumers/consumer-updates/help-stop-spread-coronavirus-and-protect-your-family>) and the importance of getting your flu vaccine (</consumers/consumer-updates/its-good-time-get-your-flu-vaccine>).

Q: Should I wear a face covering or mask when I go out in public?

A: The CDC recommends wearing masks in public when other social distancing measures are difficult to maintain.

The FDA has authorized the emergency use of face masks, including cloth face coverings, that meet certain criteria for use as source control by the general public and health care personnel in accordance with CDC recommendations during the COVID-19 public health emergency. The FDA also regulates other medical devices, including personal protective equipment (PPE) such as surgical masks and N95 respirators. The CDC recommends that PPE should be reserved for use by health care workers, first responders, and other frontline workers whose jobs put them at much greater risk of acquiring COVID-19.

Read more about types of face masks and the FDA's emergency use authorization (</medical-devices/personal-protective-equipment-infection-control/n95-respirators-surgical-masks-and-face-masks>) for non-surgical face masks.

Q: What treatments are available for COVID-19?

A: On October 22, 2020, the FDA approved the antiviral drug Veklury (remdesivir) for use in adults and pediatric patients (12 years of age and older and weighing at least 40 kg) for the treatment of COVID-19 requiring hospitalization. Veklury should only be administered in a hospital or in a healthcare setting capable of providing acute care comparable to inpatient hospital care.

This approval does not include the entire population that had been authorized to use Veklury under an Emergency Use Authorization (EUA) originally issued on May 1, 2020. In order to ensure continued access to the pediatric population previously covered under the EUA, the FDA revised the EUA for Veklury to permit the drug's use by licensed healthcare providers for the treatment of suspected or laboratory-confirmed COVID-19 in hospitalized pediatric patients 3.5 kg to less than 40 kg **or** hospitalized pediatric patients less than 12 years of age weighing at least 3.5 kg. For additional information on the authorized use of Veklury under the EUA, refer to the Fact Sheet for Healthcare Providers (</media/137566/download>).

Clinical trials assessing the safety and efficacy of Veklury (remdesivir) in this pediatric patient population are ongoing.

The National Institutes of Health provides more information about treatment options (<https://www.covid19treatmentguidelines.nih.gov/>).

People with COVID-19 should receive supportive care to help relieve symptoms. People with mild symptoms are able to recover at home. If you experience a medical emergency such as trouble breathing, call 911 and let the operator know you may have COVID-19. Never take a prescription medicine or drug if it is not prescribed for you by your doctor for your health condition.

Q: Can I prevent or treat COVID-19 by using disinfectant sprays, wipes, or liquids on my skin? Can I inject, inhale, or ingest (swallow) disinfectants to prevent or treat COVID-19?

A: No. **Disinfectants should not be used on human or animal skin.** Disinfectants may cause serious skin and eye irritation.

Disinfectants are dangerous for people to inject, inhale, or ingest. If you breathe, inject, or swallow disinfectants you may be seriously hurt or die. If someone near you swallows, injects, or breathes a disinfectant, call poison control or a medical professional immediately.

Disinfectant products such as sprays, mists, wipes, or liquids are only to be used on hard, non-porous surfaces (materials that do not absorb liquids easily) such as floors and countertops, or on soft surfaces such as mattresses, sofas, and beds.

View the current list of disinfectants that meet EPA’s criteria for use against SARS-CoV-2 (<https://www.epa.gov/pesticide-registration/list-n-disinfectants-use-against-sars-cov-2>), the virus that causes COVID-19.

Q: Does spraying people with disinfectant lower the spread of COVID-19?

A: Currently there are no data showing that spraying people with aerosolized disinfectants, or having people walk through tunnels or rooms where disinfectant is in the air, can treat, prevent, or lower the spread of COVID-19.

Surface disinfectants should **not** be used on people or animals. Disinfectant products, such as sprays, mists, wipes, or liquids are only to be used on hard, non-porous surfaces (materials that do not absorb liquids easily) such as floors and countertops, or on soft surfaces such as mattresses, sofas, and beds. CDC provides information regarding disinfectant practices for surfaces in the Reopening Guidance for Cleaning and Disinfecting Public Spaces, Workplaces, Businesses, Schools, and Homes (<https://www.cdc.gov/coronavirus/2019-ncov/community/reopen-guidance.html>).

Human antiseptic drugs, such as hand sanitizers, are intended for use on human skin, but are not intended for aerosolization (to be sprayed in the air in very small droplets). Due to serious safety concerns, including the risk of inhalational toxicity and flammability, the FDA’s temporary policies (</drugs/coronavirus-covid-19-drugs/hand-sanitizers-covid-19>) for alcohol-based hand sanitizers during the COVID-19 public health emergency specifically do not apply to aerosol sprays. In addition, hand sanitizers are intended for use on the hands, and should never be used over larger body surfaces, swallowed, or inhaled.

Q: Will Miracle Mineral Solution (MMS) cure COVID-19?

A: No. Miracle Mineral Solution does not cure COVID-19 and has not been approved by the FDA for any use. The solution, when mixed as directed, forms industrial bleach that may cause serious and potentially life-threatening side effects. FDA took action (</inspections-compliance-enforcement-and-criminal-investigations/warning-letters/genesis-2-church-606459-04082020>) against Genesis II Church of Health and Healing for unlawfully distributing Miracle Mineral Solution for the treatment of COVID-19 and other diseases. Learn more: [Danger: Don’t Drink Miracle Mineral Solution or Similar Products](/consumers/consumer-updates/danger-dont-drink-miracle-mineral-solution-or-similar-products) (</consumers/consumer-updates/danger-dont-drink-miracle-mineral-solution-or-similar-products>).

Q: Is hand sanitizer effective against COVID-19?

A: The best way to prevent the spread of infections and decrease the risk of getting sick is by washing your hands with plain soap and water, advises the CDC (<https://www.cdc.gov/handwashing/>). Washing hands often with soap and water for at least 20 seconds is essential, especially after going to the bathroom; before eating; and after coughing, sneezing, or blowing one's nose. If soap and water are not available, CDC recommends consumers use an alcohol-based hand sanitizer that contains at least 60% alcohol.

Q: Where can I buy hand sanitizer? Can I make my own hand sanitizer?

A: Many retail stores and pharmacies sell hand sanitizers. However, we understand that many stores may not have hand sanitizers available to buy. To help increase the availability of hand sanitizers, the FDA has issued guidance (</regulatory-information/search-fda-guidance-documents/guidance-industry-temporary-policy-preparation-certain-alcohol-based-hand-sanitizer-products-during>) for the temporary preparation of alcohol-based hand sanitizers by some companies and pharmacies during the COVID-19 public health emergency.

The FDA does not recommend that consumers make their own hand sanitizer. If made incorrectly, hand sanitizer can be ineffective, and there have been reports of skin burns from homemade hand sanitizer. The agency lacks verifiable information on the methods being used to prepare hand sanitizer at home and whether they are safe for use on human skin.

See the Q&A for Consumers: Hand Sanitizers and COVID-19 (</drugs/information-drug-class/qa-consumers-hand-sanitizers-and-covid-19>) and Safely Using Hand Sanitizer (</consumers/consumer-updates/safely-using-hand-sanitizer>) for more information.

Q: What do I do if I get a rash or other reaction to hand sanitizer?

A: Call your doctor if you experience a serious reaction to hand sanitizer. The FDA encourages consumers and health care professionals to report adverse events experienced with the use of hand sanitizers to the FDA's MedWatch Adverse Event Reporting (</safety/medwatch-fda-safety-information-and-adverse-event-reporting-program>) program:

- Complete and submit the report online (<https://www.accessdata.fda.gov/scripts/medwatch/index.cfm>); or
- Download and complete the form (</media/76299/download>), then submit it via fax at 1-800-FDA-0178.
- Include as much information as you can about the product that caused the reaction, including the product name, the manufacturer, and the lot number (if available).

See Q&A for Consumers: Hand Sanitizers and COVID-19 (</drugs/information-drug-class/qa-consumers-hand-sanitizers-and-covid-19>) and Safely Using Hand Sanitizer (<https://www.fda.gov/consumers/consumer-updates/safely-using-hand-sanitizer>) for more information.

Q: What is the risk of using a hand sanitizer that contains methanol (wood alcohol) or 1-propanol?

A: Methanol exposure can result in nausea, vomiting, headache, blurred vision, permanent blindness, seizures, coma, permanent damage to the nervous system or death. Although people using these products on their hands are at risk for methanol poisoning, young children who accidentally swallow these products and adolescents and adults who drink these products as an alcohol (ethanol) substitute are most at risk.

Swallowing or drinking a hand sanitizer with 1-propanol can result in decreased breathing and heart rate, among other serious symptoms, and can lead to death. Hand sanitizer with 1-propanol contamination can irritate your skin (or eyes, if exposed). Although it is rare, some people have reported allergic skin reactions. Learn more about methanol and 1-propanol toxicities (</consumers/consumer-updates/your-hand-sanitizer-fdas-list-products-you-should-not-use>).

Q: What should I do with hand sanitizer that contains methanol (wood alcohol) or 1-propanol?

A: If you have one of the products the FDA's do-not-use list of hand sanitizers (</drugs/drug-safety-and-availability/fda-updates-hand-sanitizers-methanol#products>), you should immediately stop using it and dispose of the product, ideally in a hazardous waste container (<https://www.epa.gov/hw/household-hazardous-waste-hhw>). Do not pour these products down the drain or flush them. Contact your local waste management and recycling center (<https://www.epa.gov/hwgenerators/links-hazardous-waste-programs-and-us-state-environmental-agencies>) for more information on hazardous waste

disposal. Learn how to search FDA's hand sanitizer do-not-use list, including a description of how to search for manufacturers and distributors on the label (</consumers/consumer-updates/your-hand-sanitizer-fdas-list-products-you-should-not-use>).

Q: What should people do if they have been exposed to hand sanitizer with potential methanol or 1-propanol contamination?


A: People who have been exposed to contaminated hand sanitizer and are experiencing symptoms should seek immediate medical treatment for potential reversal of toxic effects.

FDA encourages health care professionals, consumers and patients to report adverse events or quality problems experienced with the use of hand sanitizers to FDA's MedWatch Adverse Event Reporting program (</safety/medwatch-fda-safety-information-and-adverse-event-reporting-program>) (please provide the agency with as much information as possible to identify the product):

- Complete and submit the report online (<https://www.accessdata.fda.gov/scripts/medwatch/index.cfm>); or
- Download and complete the form (</media/85598/download>), then submit it via fax at 1-800-FDA-0178.

Q: Products online claim to prevent or treat COVID-19. Where can I report websites selling products with fraudulent claims?

A: The FDA advises consumers to be beware of websites and stores selling products that claim to prevent, treat, or cure COVID-19. If you have a question about a product sold online that claims to treat, prevent, or cure COVID-19, talk to your health care provider or doctor.

Watch this video (<https://youtu.be/YXntX39C1rg>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>) and read this Consumer Update (</consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments>) to learn how to protect yourself and your family from coronavirus fraud.

Please report websites (<https://www.accessdata.fda.gov/scripts/email/oc/buyonline/english.cfm>) selling products with fraudulent claims about treatment or prevention of COVID-19. If you have experienced a bad reaction to a product sold with COVID-19 claims, report it to the FDA's MedWatch Adverse Event Reporting program:

- Complete and submit the report online (<https://www.accessdata.fda.gov/scripts/medwatch/index.cfm>); or
- Download and complete the form (</media/76299/download>), then submit it via fax at 1-800-FDA-0178.

Include as much information as you can about the product that caused the reaction, including the product name, the manufacturer, and the lot number (if available).

Q: Am I at risk for serious complications from COVID-19 if I smoke cigarettes?

A: Yes. Data shows that when compared to never smokers, cigarette smoking increases the risk of more severe illness from COVID-19, which could result in hospitalization, the need for intensive care, or even death. Smoking cigarettes can cause inflammation and cell damage throughout the body, and can weaken your immune system, making it less able to fight off disease.

There's never been a better time to quit smoking. If you need resources to help you quit smoking, the FDA's Every Try Counts (<https://smokefree.gov/everytrycounts/>) campaign has supportive tips and tools to help you get closer to quitting for good.

Q: If I vape tobacco or nicotine am I at risk for complications from COVID-19?

A: E-cigarette use can expose the lungs to toxic chemicals, but whether those exposures increase the risk of COVID-19 or the severity of COVID-19 outcomes is not known. However, many e-cigarette users are current or former smokers, and cigarette smoking increases the risk of respiratory infections, including pneumonia.

Vaccines, Biologics, Human Tissues, and Blood Products

Q: What is the FDA's role in approving vaccines and what is being done to produce a COVID-19 vaccine?

A: The FDA regulates vaccines. Vaccines undergo a rigorous review of laboratory, clinical, and manufacturing data to ensure the safety and effectiveness of these products. Vaccines approved for marketing may also be required to undergo additional studies to further

evaluate the vaccine and often to address specific questions about the vaccine's safety, effectiveness, or possible side effects.

On December 11, 2020, the FDA issued an Emergency Use Authorization (EUA) for the use of the Pfizer-BioNTech COVID-19 Vaccine ([/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/pfizer-biontech-covid-19-vaccine](#)). On December 18, 2020, the FDA issued an EUA for the use of the Moderna COVID-19 Vaccine ([/emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/moderna-covid-19-vaccine](#)). The issuance of an EUA is different than an FDA approval (licensure) of a vaccine.

In determining whether to issue an EUA for a product, the FDA evaluates the available evidence and assesses any known or potential risks and any known or potential benefits. And if the benefit-risk assessment is favorable, the product is made available during the public health emergency. Once a manufacturer submits an EUA request for a COVID-19 vaccine, the FDA then evaluates the request and determines whether the relevant statutory criteria are met, taking into account the totality of the scientific evidence about the vaccine that is available to the agency.

In addition to supporting product development for high priority COVID-19 vaccines, the FDA continues to expedite clinical trials for additional vaccine candidates, providing timely advice to and interactions with vaccine developers.

Vaccine developers can find more information about the review process here ([/vaccines-blood-biologics/industry-biologics/coronavirus-covid-19-cber-regulated-biologics](#)).

Q: What is a biological medical product or a biologic?


A: Biological products include a wide range of products such as vaccines, blood and blood components, allergenics, somatic cells, gene therapy, tissues, and recombinant therapeutic proteins. Biologics can be composed of sugars, proteins, or nucleic acids or complex combinations of these substances, or may be living entities such as cells and tissues.

Q: Are there any vaccines or other medical products available to prevent COVID-19?

A: Yes. On December 11, 2020 the FDA issued the first Emergency Use Authorization for a COVID-19 vaccine, and on December 18, 2020, authorized a second COVID-19 vaccine.

Additionally, the FDA is working with other vaccine developers, researchers, and manufacturers to help expedite the development and availability of medical products such as additional vaccines, monoclonal antibodies, and other drugs to prevent or treat COVID-19.

Read more (</vaccines-blood-biologics/industry-biologics/coronavirus-covid-19-cber-regulated-biologics>) about what the FDA is doing to mitigate the effects of COVID-19.

For information about vaccine clinical trials for COVID-19 visit clinicaltrials.gov (<https://clinicaltrials.gov/>) and the COVID-19 Prevention Network (<https://www.coronaviruspreventionnetwork.org/>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>). Note: The information on clinicaltrials.gov is provided by the sponsor or principal investigator of a clinical trial. The listing of a study on the site does not reflect evaluation or endorsement of the trial by the Federal government.

Q: Can the FDA help me get a COVID-19 vaccine?

A: No. The FDA's authority includes authorizing or approving COVID-19 vaccines for use in the United States, but the FDA is not responsible for vaccine distribution. Go to the CDC website (<https://www.cdc.gov/coronavirus/2019-ncov/vaccines/index.html>) to find your state and local health departments who are responsible for COVID-19 vaccine distribution. All questions and concerns should be sent to your state government or local health department. The U.S. government's goal is to have enough COVID-19 vaccine doses for all people in the United States who choose to be vaccinated.

If you are contacted directly by someone who says they are from the FDA about a COVID-19 vaccine appointment, it is a scam. The Federal Trade Commission has easy tips on how to avoid (https://www.ftc.gov/sites/default/files/u544718/covid-vaccine-scams_infographic.jpg) COVID-19 vaccine scams. The FDA encourages you to report a potential COVID-19 drug or medical product scam on our website (<https://www.accessdata.fda.gov/scripts/email/oc/buyonline/english.cfm>).

Q: Does COVID-19 present a risk to the safety of the nation's blood supply?

A: In general, respiratory viruses are not known to be transmitted by blood transfusion, and there have been no reported cases of transfusion-transmitted coronavirus.

Q: Can SARS-CoV-2, the virus that causes COVID-19, be transmitted by blood transfusion?

A: In general, respiratory viruses are not known to be transmitted by blood transfusion, and there have been no reported cases of transfusion-transmitted coronavirus.

Q: What steps are being taken to protect the U.S. blood supply from SARS-CoV-2, the virus that causes COVID-19?

A: Blood donors must be healthy and feel well on the day of donation. Routine blood donor screening measures that are already in place should prevent individuals with respiratory infections from donating blood. For example, blood donors must be in good health and have a normal temperature on the day of donation.

Donors are instructed to contact the donor center if they become ill after donation, so that their blood or plasma will not be used. Even when a donor develops COVID-19 after donation, however, there have been no cases of COVID-19 linked to donor blood or products made from blood.


The FDA has provided additional information to blood establishments ([/vaccines-blood-biologics/safety-availability-biologics/updated-information-blood-establishments-regarding-covid-19-pandemic-and-blood-donation](#)) on its website.

Q: Why aren't blood centers testing donors for SARS-CoV-2?


A: At this time, the FDA does not recommend using laboratory tests to screen blood. Someone who has symptoms of COVID-19, including fever, cough, and shortness of breath, is not healthy enough to donate blood. Standard screening processes already in place will mean that someone with these symptoms will not be allowed to donate.

Q: Is it safe for me to donate blood during the coronavirus pandemic?

A: If you are healthy and interested in donating blood, the FDA encourages you to contact a local donation center to make an appointment. One way to make a difference during a public health emergency is to donate blood if you are able.

- AABB: www.aabb.org (<http://www.aabb.org/Pages/default.aspx>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>);

+1.301.907.6977

- America's Blood Centers: www.americasblood.org (<https://americasblood.org/>) 
(<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)
- American Red Cross: www.redcrossblood.org (<https://www.redcrossblood.org/>) 
(<http://www.fda.gov/about-fda/website-policies/website-disclaimer>); +1.800.RED
CROSS (+1.800.733.2767)
- Armed Services Blood Program: www.militaryblood.dod.mil
(<https://www.militaryblood.dod.mil/>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>); +1.703.681.8024
- Blood Centers of America: www.bca.coop (<http://bca.coop/>) 
(<http://www.fda.gov/about-fda/website-policies/website-disclaimer>)


Q: Can COVID-19 be transmitted through human cells, tissues, or cellular and tissue-based products (HCT/Ps)?

A: Respiratory viruses, in general, are not known to be transmitted by implantation, transplantation, infusion, or transfer of human cells, tissues, or cellular or tissue-based products (HCT/Ps). The potential for transmission of COVID-19 by HCT/Ps is unknown at this time. There have been no reported cases of transmission of COVID-19 via HCT/Ps.

Routine screening measures are already in place for evaluating clinical evidence of infection in HCT/P donors. Read more about HCT/Ps (</vaccines-blood-biologics/safety-availability-biologics/updated-information-human-cell-tissue-or-cellular-or-tissue-based-product-http-establishments>).

Q: What is convalescent plasma and why is it being investigated to treat COVID-19?

A: Convalescent refers to anyone recovering from a disease. Plasma is the yellow, liquid part of blood that contains antibodies. Antibodies are proteins made by the body in response to infections. Convalescent plasma from patients who have already recovered from coronavirus disease 2019 (COVID-19) may contain antibodies against COVID-19. The FDA has issued an emergency use authorization (</emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization#coviddrugs>) for the use of convalescent plasma in hospitalized patients. It is being investigated (</vaccines-blood-biologics/investigational-new-drug-ind-or-device-exemption-ide-process-cber/recommendations-investigational-covid-19-convalescent-plasma>) for the treatment of COVID-19 patients. Based on scientific evidence available, the FDA concluded this product may be effective in treating COVID-19 and that the known and potential benefits of the

product outweigh the known and potential risks of the product for patients hospitalized with COVID-19. Learn more about donating from this video (<https://youtu.be/BydAsLSNZ8o>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>).

Q: I recently recovered from COVID-19, can I donate convalescent plasma?

A: COVID-19 convalescent plasma must only be collected from recovered individuals if they are eligible to donate blood. Individuals must have had a prior diagnosis of COVID-19 documented by a laboratory test and meet other laboratory criteria. Individuals must have fully recovered from COVID-19, with complete resolution of symptoms for at least 14 days before donation of convalescent plasma. You can ask your local blood center if there are options to donate convalescent plasma in your area. Learn more about how to donate (</emergency-preparedness-and-response/coronavirus-disease-2019-covid-19/donate-covid-19-plasma>).

Drugs (Medicines)

Q: What does it mean to be an FDA-approved drug?

A: FDA approval of a drug means that the agency has determined, based on substantial evidence, that the drug is effective for its intended use, and that the benefits of the drug outweigh its risks when used according to the product's approved labeling. The drug approval process takes place within a structured framework that includes collecting clinical data and submitting an application to the FDA. Learn more about the FDA's Drug Review Process (</drugs/information-consumers-and-patients-drugs/fdas-drug-review-process-ensuring-drugs-are-safe-and-effective>).

Q: What is the FDA's role in regulating potential treatments during a public health emergency?

A: The FDA carries out many activities to protect and promote public health during a public health emergency, including helping to accelerate the development and availability of potential treatments, protecting the security of drug supply chains, providing guidance to food and medical device manufacturers, advising developers on clinical trial issues, and keeping the public informed with authoritative health information.

The FDA is committed to supporting the development of new drugs, and the potential repurposing of existing drugs, to address COVID-19 by working with potential drug makers and sponsors to rapidly move products into clinical trials, helping to ensure that trials are properly designed and safe, and protecting the public from potentially unsafe products.

Read more about FDA efforts to accelerate treatments (</drugs/coronavirus-covid-19-drugs/coronavirus-treatment-acceleration-program-ctap>) and other actions related to coronavirus (</drugs/coronavirus-covid-19-drugs/cders-work-protect-public-health-during-covid-19-public-health-emergency>).

Q: Are there any FDA-approved drugs (medicines) for COVID-19?

A: Yes, the FDA has approved Veklury (remdesivir) for certain COVID-19 patients. Read more about the approval here (</news-events/press-announcements/fda-approves-first-treatment-covid-19>).

Additionally, during public health emergencies, the FDA may in certain circumstances authorize use of unapproved drugs or unapproved uses of approved drugs for life-threatening conditions when there are no adequate, approved, and available options and other conditions are met. This is called an Emergency Use Authorization (EUA) (</emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization#coviddrugs>).

Researchers are studying new drugs, and medicines that are already approved for other health conditions, as possible treatments for COVID-19. The FDA created the Coronavirus Treatment Acceleration Program (CTAP) (</drugs/coronavirus-covid-19-drugs/coronavirus-treatment-acceleration-program-ctap>) to use every available method to move new treatments to patients. Additionally, the FDA is working with the National Institutes of Health (<https://www.nih.gov/research-training/medical-research-initiatives/activ>), drug manufacturers, researchers, and other partners (<https://covid19.reaganudall.org/covid-19-hub>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>) to accelerate the development process for COVID-19 treatments. FDA's Sentinel System (<https://www.sentinelinitiative.org/drugs/fda-sentinel-system-coronavirus-covid-19-activities>) [↗](http://www.fda.gov/about-fda/website-policies/website-disclaimer) (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>) is being used to monitor the use of drugs, describe the course of illness among hospitalized patients, and evaluate the treatment impact of therapies actively being used under real-world conditions.

For information about clinical trials for COVID-19 treatments visit clinicaltrials.gov (<https://clinicaltrials.gov/>) and the COVID-19 Prevention Network (<https://www.coronaviruspreventionnetwork.org/>) [↗](http://www.fda.gov/about-) (

fda/website-policies/website-disclaimer). Note: The information on clinicaltrials.gov is provided by the sponsor or principal investigator of a clinical trial. The listing of a study on the site does not reflect evaluation or endorsement of the trial by the Federal government.

Q: Is Veklury (remdesivir) approved by the FDA to treat COVID-19?

A: Yes, on October 22, 2020, the FDA approved Veklury (remdesivir) for certain COVID-19 patients. Read more about the approval here (</news-events/press-announcements/fda-approves-first-treatment-covid-19>).

Q: Is Olumiant (baricitinib) approved by the FDA to treat COVID-19?

A: No. Olumiant is not FDA-approved for the treatment of COVID-19. However, the FDA issued an emergency use authorization (EUA) authorizing Olumiant for emergency use by healthcare providers, in combination with Veklury (remdesivir), for the treatment of suspected or laboratory-confirmed COVID-19 in hospitalized adults and pediatric patients 2 years of age or older requiring supplemental oxygen, invasive mechanical ventilation, or extracorporeal membrane oxygenation (ECMO).

For more information see Frequently Asked Questions on the Emergency Use Authorization for Olumiant (baricitinib) in Combination with Veklury (remdesivir) for Treatment of Mild to Moderate COVID-19 (</media/143825/download>).

Q: Is bamlanivimab, a monoclonal antibody, FDA-approved to treat COVID-19?

A: No. Bamlanivimab is not FDA-approved to treat any diseases or conditions, including COVID-19. However, the FDA issued an emergency use authorization (EUA) for bamlanivimab for the treatment of mild to moderate COVID-19 in adults and pediatric patients with positive results of direct SARS-CoV-2 viral testing who are 12 years and older weighing at least 40kg, and who are at high risk for progressing to severe COVID-19 and/or hospitalization. Learn more about bamlanivimab for COVID-19 (</emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization#coviddrugs>).

Q: Are the monoclonal antibodies, casirivimab and imdevimab, FDA-approved to treat COVID-19?

A: No. Casirivimab and imdevimab are not FDA-approved to treat any diseases or conditions, including COVID-19. However, the FDA issued an emergency use authorization (EUA) for casirivimab and imdevimab to be administered together for the treatment of mild to moderate COVID-19 in adults and pediatric patients (12 years of age or older weighing at least 40 kilograms [about 88 pounds]) with positive results of direct SARS-CoV-2 viral testing and who are at high risk for progressing to severe COVID-19. This includes those who are 65 years of age or older or who have certain chronic medical conditions. Learn more about casirivimab and imdevimab for COVID-19 (</news-events/press-announcements/coronavirus-covid-19-update-fda-authorizes-monoclonal-antibodies-treatment-covid-19>).

Q: What is a monoclonal antibody?

A: Monoclonal antibodies are laboratory-produced molecules that act as substitute antibodies that can restore, enhance or mimic the immune system's attack on cells. Monoclonal antibodies for COVID-19 may block the virus that causes COVID-19 from attaching to human cells, making it more difficult for the virus to reproduce and cause harm. Monoclonal antibodies may also neutralize a virus.

Q: Are chloroquine phosphate or hydroxychloroquine sulfate approved by the FDA to treat COVID-19?

A: No. Hydroxychloroquine sulfate and some versions of chloroquine phosphate are FDA-approved to treat malaria. Hydroxychloroquine sulfate is also FDA-approved to treat lupus and rheumatoid arthritis.

On March 28, 2020, the FDA issued an emergency use authorization (EUA) (</emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization-archived-information#covid19>) for chloroquine phosphate and hydroxychloroquine sulfate to treat adults and adolescents hospitalized with COVID-19 for whom a clinical trial was not available or participation was not feasible. Based on FDA's continued review of the scientific evidence available, the criteria for an EUA for chloroquine phosphate and hydroxychloroquine sulfate as outlined in Section 564(c)(2) of the FD&C Act are no longer met. As a result, the EUA for these two drugs was revoked on June 15, 2020. Read more about this action (</media/138946/download>).

Q: Should I take chloroquine phosphate used to treat disease in aquarium fish to prevent or treat COVID-19?

A: No. Products marketed for veterinary use, “for research only,” or otherwise not for human consumption have not been evaluated for safety or effectiveness and **should never be used by humans**. The FDA is aware that chloroquine phosphate is marketed to treat disease in aquarium fish, but these products have not been evaluated by the FDA to determine if they are safe, effective, properly manufactured, and adequately labeled. The agency continues to work with online marketplaces to remove these items, and many have been removed based on these efforts. Patients should not take any form of chloroquine unless it has been prescribed by a licensed health care provider. Chloroquine products also should not be given to pets or livestock unless prescribed by a veterinarian.


Q: Are antibiotics effective in preventing or treating COVID-19?

A: No. Antibiotics do not work against viruses; they only work on bacterial infections. Antibiotics do not prevent or treat COVID-19, because COVID-19 is caused by a virus, not bacteria. Some patients with COVID-19 may also develop a bacterial infection, such as pneumonia. In that case, a health care professional may treat the bacterial infection with an antibiotic.

Q: Should I take ivermectin to prevent or treat COVID-19?

A: No. While there are approved uses for ivermectin in people and animals, it is not approved for the prevention or treatment of COVID-19. You should not take any medicine to treat or prevent COVID-19 unless it has been prescribed to you by your health care provider and acquired from a legitimate source.

A recently released research article

(<https://www.sciencedirect.com/science/article/pii/S0166354220302011>) 

(<http://www.fda.gov/about-fda/website-policies/website-disclaimer>) described the effect of ivermectin on SARS-CoV-2 in a laboratory setting. These types of laboratory studies are commonly used at an early stage of drug development. Additional testing is needed to determine whether ivermectin might be appropriate to prevent or treat coronavirus or COVID-19. Read more about ivermectin (</animal-veterinary/product-safety-information/faq-covid-19-and-ivermectin-intended-animals>).

Q: What is the FDA doing to protect people from products making fraudulent COVID-19 claims?

A: We have established a cross-agency team dedicated to closely monitoring for fraudulent COVID-19 products (</consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products>). In response to internet scammers, the FDA has taken – and continues to take – actions to stop those selling unapproved products that fraudulently claim to prevent, treat, diagnose or cure COVID-19. The FDA and the Federal Trade Commission (FTC) issue warning letters to companies and individuals that are unlawfully selling unapproved products with fraudulent COVID-19 claims. The FDA also has taken enforcement action against certain sellers that continued to illegally market products for prevention or treatment of COVID-19.

Additionally, the FDA also has reached out to major retailers to ask for their help in monitoring online marketplaces for fraudulent COVID-19 products. You can report websites selling fraudulent medical products (</safety/report-problem-fda/reporting-unlawful-sales-medical-products-internet>) to the FDA through our website, by phone at 1-800-332-1088, or email to FDA-COVID-19-Fraudulent-Products@fda.hhs.gov (mailto:FDA-COVID-19-Fraudulent-Products@fda.hhs.gov). Read more in the consumer update on fraudulent products (</consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments>).

Q: Will there be drug shortages due to COVID-19?

A: The FDA has been closely monitoring the supply chain with the expectation that the COVID-19 outbreak would likely impact the medical product supply chain, including potential disruptions to supply or shortages of critical medical products in the U.S.

We have been reaching out to manufacturers as part of our approach to identifying potential disruptions or shortages. We will use all available tools to react swiftly and mitigate the impact to U.S. patients and health care professionals when a potential disruption or shortage is identified.

Find real-time information

(<https://www.accessdata.fda.gov/scripts/drugshortages/default.cfm>) about drug shortages.

Learn more in our drug shortages frequently asked questions (</drugs/drug-shortages/frequently-asked-questions-about-drug-shortages>).

Q: Am I at risk for COVID-19 from taking FDA-approved drugs made outside the United States?

A: Currently, there is no evidence to support transmission of COVID-19 associated with imported goods, including food and drugs for humans and pets. There have not been any cases of COVID-19 in the United States associated with imported goods. Learn more about the FDA's Import Program (</industry/import-program-food-and-drug-administration-fda>) and Importing COVID Supplies (</industry/import-program-food-and-drug-administration-fda/importing-covid-19-supplies>).

Q: Who should I contact with drug-related questions?

A: If you have additional questions, call the FDA's Division of Drug Information at (855) 543-3784 or email us at druginfo@fda.hhs.gov (<mailto:druginfo@fda.hhs.gov>).

Medical Devices Including Tests for COVID-19

Q: Is there a test for COVID-19?

A: Yes, the FDA has issued Emergency Use Authorizations (EUAs) (</emergency-preparedness-and-response/mcm-legal-regulatory-and-policy-framework/emergency-use-authorization#covidinvitrodev>) for different types of COVID-19 tests. Some tests are used to diagnose the virus that causes COVID-19 infection whereas other tests are used to detect a recent or prior COVID-19 infection. There are 2 different types of COVID-19 diagnostic tests -- molecular tests and antigen tests. Molecular tests detect the virus that causes COVID-19, SARS-CoV-2. Antigen tests detect specific proteins made by the virus. Tests that detect recent or prior COVID-19 infection are called antibody or serology tests. The EUAs allow the emergency use of tests during the COVID-19 emergency when the FDA determines certain criteria are met. These criteria include that the test may be effective at diagnosing COVID-19 and that the known and potential benefits outweigh the known and potential risks. Read more about COVID-19 tests (</medical-devices/emergency-situations-medical-devices/coronavirus-covid-19-and-medical-devices#IVD>) and find a community-based testing site (<https://www.hhs.gov/coronavirus/community-based-testing-sites/index.html>).

Q: How are people tested for COVID-19?

A: Most tests to diagnose COVID-19 require a swab of your nose, or the part of the throat behind the nose, by a health care provider. Some tests use saliva (spit) or other types of collection methods. For most tests, the swab or sample must be sent to a lab for analysis. Some tests allow the patient to collect the sample at home and then send it to a lab for analysis. Some tests can be analyzed at the point-of-care, such as in a doctor's office or health clinic. The FDA has also authorized some at-home tests that allow a person to collect their sample and run the test completely at home without sending anything to a lab. Some tests can be purchased online or in a store without a prescription, but they may not be available everywhere. Learn more about Coronavirus Disease 2019 Testing Basics (</consumers/consumer-updates/coronavirus-disease-2019-testing-basics>).

Q: Are there any at-home tests for COVID-19?

A: Yes. There are now COVID-19 tests available for purchase online or in a store that can be used completely at home. At-home tests allow you to collect your own sample and test it with a system that gives you results in minutes at home.

Additionally, the FDA has authorized some tests that can be purchased online or in a store that allow you to collect your own sample and then send it to a laboratory for analysis.

Q: When will other diagnostic tests for COVID-19 be authorized?

A: The FDA is actively working with test developers and issues Emergency Use Authorizations (EUAs) frequently for EUA requests with sufficient supporting data.

Q: What is the difference between the types of tests available for SARS-CoV-2?

A: There are two different types of tests – **diagnostic tests** and **antibody tests**.

1. A **diagnostic test** can show if you have an active coronavirus infection and should take steps to quarantine or isolate yourself from others. Currently there are two types of diagnostic tests – **molecular (RT-PCR)** tests that detect the virus's genetic material, and **antigen** tests that detect specific proteins on the surface of the virus. Samples are typically collected with a nasal or throat swab, or saliva collected by spitting into a tube.
2. An **antibody test** looks for antibodies that are made by the immune system in response to a threat, such as a specific virus. Antibodies can help fight infections. Antibodies can take several days or weeks to develop after you have an infection and

may stay in your blood for several weeks after recovery. Because of this, antibody tests should not be used to diagnose an active coronavirus infection. At this time, researchers do not know if the presence of antibodies means that you are immune to the coronavirus in the future. While there is a lot of uncertainty with this new virus, it is also possible that, over time, broad use of antibody tests and clinical follow-up will provide the medical community with more information on whether or not, and how long, a person who has recovered from the virus is at lower risk of infection if they are exposed to the virus again. Samples are typically blood from a finger stick or blood draw. Learn more about antibody tests (</medical-devices/coronavirus-covid-19-and-medical-devices/antibody-serology-testing-covid-19-information-patients-and-consumers>).

Learn more about the different types of tests and the steps involved (</consumers/consumer-updates/coronavirus-disease-2019-testing-basics>) in the FDA's Consumer Update on Coronavirus Testing Basics.

Q: Should I purchase personal protective equipment such as facemasks or N95 respirators for me and my family?

A: No. Surgical masks and N95s (</medical-devices/personal-protective-equipment-infection-control/n95-respirators-surgical-masks-and-face-masks>) need to be reserved for use by health care workers, first responders, and other frontline workers whose jobs put them at much greater risk of acquiring COVID-19. The cloth face coverings recommended by CDC are not surgical masks or N95 respirators. Surgical masks and N95s are critical supplies that must continue to be reserved for health care workers and other medical first responders, as recommended by CDC.

Q: Is there a shortage of personal protective equipment (PPE) such as gloves, masks, and N95 respirators or of ventilators?

A: The FDA has been working closely with PPE and ventilator manufacturers to understand their supply capabilities during this pandemic. The agency is also aware of challenges throughout the supply chain that are presently impacting the availability of PPE products and is taking steps to mitigate shortages that health care facilities are already experiencing.

The FDA issued new guidance (</news-events/press-announcements/coronavirus-covid-19-update-fda-continues-facilitate-access-crucial-medical-products-including>) to give ventilator manufacturers and non-medical device manufacturers more flexibility to start making new ventilators and parts. We adjusted our screening of PPE and medical devices

(/news-events/press-announcements/coronavirus-covid-19-update-fda-takes-action-increase-us-supplies-through-instructions-ppe-and) at U.S. ports of entry to expedite imports of legitimate products into the U.S. With CDC we took action (/news-events/press-announcements/coronavirus-covid-19-update-fda-and-cdc-take-action-increase-access-respirators-including-n95s) to make more respirators, including certain N95s, available to health care personnel for use in health care settings. Read more about PPE (/medical-devices/emergency-situations-medical-devices/coronavirus-covid-19-and-medical-devices#PPE).

The FDA encourages manufacturers and health care facilities to report any supply disruptions to the device shortages mailbox at deviceshortages@fda.hhs.gov (mailto:deviceshortages@fda.hhs.gov).

Q: Can 3D printing be used to make PPE?

A: Personal protective equipment (PPE) includes protective clothing, gowns, gloves, face shields, goggles, face masks, and respirators or other equipment designed to protect the wearer from injury or the spread of infection or illness. While it is possible to use 3D printing to make certain PPE, there are technical challenges. 3D-printed PPE may provide a physical barrier, but 3D-printed PPE are unlikely to provide the same fluid barrier and air filtration protection as FDA-cleared surgical masks and N95 respirators. The CDC has recommendations for how to optimize the supply of face masks (<https://www.cdc.gov/coronavirus/2019-ncov/hcp/ppe-strategy/face-masks.html>). Find more information about 3D printing during the COVID-19 pandemic (/medical-devices/coronavirus-covid-19-and-medical-devices/3d-printing-medical-devices-accessories-components-and-parts-during-covid-19-pandemic).

Q: I built a DIY ventilator using instructions I found on the internet. May I sell it?

A: DIY ventilator makers may request that their product be added to the Emergency Use Authorization (EUA) that the FDA issued on March 24, 2020, to legally market the product in the U.S. Instructions on how to do so, and the criteria for ventilator safety, performance and labeling, may be found in the Letter of Authorization and Appendix A for the EUA (/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/ventilators-and-ventilator-accessories-euas) related to ventilators, anesthesia gas machines modified for use as ventilators, positive pressure breathing devices modified for use as ventilators, ventilator tubing connectors, and ventilator accessories.

Q: Who should I contact if I have questions about medical devices or need more information?

A: Please see [Contacts for Medical Devices During the COVID-19 Pandemic \(/medical-devices/coronavirus-covid-19-and-medical-devices/contacts-medical-devices-during-covid-19-pandemic\)](#).

If you need information about the development of a test for SARS-CoV-2, please see our [FAQs on Testing for SARS-CoV-2 \(/medical-devices/coronavirus-covid-19-and-medical-devices/faqs-testing-sars-cov-2\)](#).

Food Products

Q: What is the FDA's role in helping to ensure the safety of the human and animal food supply?

A: To protect public health, the FDA monitors domestic firms and the foods that they produce. The FDA also monitors imported products and foreign firms exporting to the United States. The FDA protects consumers from unsafe foods through research and methods development; inspection and sampling; and regulatory and legal action.

Q: Will there be food shortages?

A: In some cases the inventory of certain foods at your grocery store might be temporarily low before stores can restock. Food production and manufacturing generally are widely dispersed throughout the U.S., however; there is a significant shift in where consumers are buying food during the pandemic. While food use in large-scale establishments, such as hotels, restaurants, sports arenas/stadiums and universities suddenly declined, the demand for food at grocery stores increased.

The FDA has issued temporary guidance ([/food/guidance-regulation-food-and-dietary-supplements/guidance-documents-regulatory-information-topic-food-and-dietary-supplements#y2020](#)) to provide flexibility in packaging and labeling requirements to support food supply chains and get foods to the consumer retail marketplace. The FDA is closely monitoring the food supply chain for any shortages in collaboration with industry and our federal and state partners. We are in regular contact with food manufacturers and grocery stores. Watch a video ([/consumers/consumer-updates/food-safety-and-availability-during-coronavirus-pandemic](#)) on food safety and availability during the coronavirus pandemic.

Q: Why is the FDA providing flexibility to food manufacturers, under limited circumstances during the COVID-19 public health emergency, to make minor changes in ingredients without reflecting those changes on the package label?

A: Due to limited shortages of specific ingredients and foods, or unexpected supply chain disruptions in some industries, food manufacturers may need to make small changes to some ingredients during the COVID-19 public health emergency. Manufacturers may not be able to relabel their products to reflect these minor changes on the food label without slowing down the processing or distribution of the food.

To avoid slowing down food processing or distribution during the coronavirus pandemic, the FDA issued a guidance titled "[Temporary Policy Regarding Certain Food Labeling Requirements During the COVID-19 Public Health Emergency: Minor Formulation Changes and Vending Machines \(/regulatory-information/search-fda-guidance-documents/temporary-policy-regarding-certain-food-labeling-requirements-during-covid-19-public-health\)](#)." The temporary policy provides food manufacturers with flexibility to make minor formulation changes in certain, limited circumstances without making conforming label changes on packages as long as any substitutions or omissions of ingredients do not pose a health or safety issue (such as allergens), and do not cause significant changes in the finished product.

Q: What do I need to know about the temporary policy for food labeling of minor ingredient changes during the COVID-19 public health emergency if I have food allergies?

A: Although the temporary policy allows some flexibility, the eight major food allergens under the Food Allergen Labeling and Consumer Protection Act (FALCPA) of 2004 ([/food/food-allergensgluten-free-guidance-documents-regulatory-information/food-allergen-labeling-and-consumer-protection-act-2004-questions-and-answers](#)) cannot be substituted for labeled ingredients by manufacturers without a corresponding label change. While the temporary policy does not list all ingredients known to cause sensitivities in some people, manufacturers should avoid substituting ingredients with major food allergens or with ingredients recognized as priority allergens (such as sesame, celery, lupin, buckwheat, molluscan shellfish, and mustard) in other parts of the world without a label change. These flexibilities are intended to remain in effect only for the duration of the COVID-19 public health emergency in the United States. However, when this public health emergency is over, extensions may be needed if the food and agriculture sectors need additional time to bring supply chains back into regular order. For more information please see more Questions and

Answers on FDA's Temporary Policy on Food Labeling Changes During the COVID-19 Pandemic (/food/food-safety-during-emergencies/questions-and-answers-fdas-temporary-policy-food-labeling-changes-during-covid-19-pandemic).

Q: Will there be animal food shortages?

A: There are no nationwide shortages of animal food, although in some cases the inventory of certain foods at your grocery store might be temporarily low before stores can restock. Animal food production and manufacturing are widely dispersed throughout the United States and no widespread disruptions have been reported in the supply chain.

Q: What are the most important things I need to know to keep myself and others safe when I go to the grocery store during the pandemic?

A: There are steps you can take to help protect yourself, grocery store workers and other shoppers, such as wearing a face covering, practicing social distancing, and using wipes on the handles of the shopping cart or basket. Read more tips in Shopping for Food During the COVID-19 Pandemic - Information for Consumers (/food/food-safety-during-emergencies/shopping-food-during-covid-19-pandemic-information-consumers).

Q: Are food products produced in the United States or other countries affected by COVID-19 a risk for the spread of COVID-19?

A: There is no evidence to suggest that food produced in the United States or imported from countries affected by COVID-19 can transmit COVID-19.

Q: Can I get the coronavirus from food, food packaging, or food containers and preparation area?

A: Currently there is no evidence of food, food containers, or food packaging being associated with transmission of COVID-19. Like other viruses, it is possible that the virus that causes COVID-19 can survive on surfaces or objects.

If you are concerned about contamination of food or food packaging, wash your hands after handling food packaging, after removing food from the packaging, before you prepare food for eating and before you eat. Consumers can follow CDC guidelines on frequent hand washing (<https://www.cdc.gov/handwashing/>) with soap and water for at least 20 seconds; and frequently clean and disinfect surfaces.

It is always important to follow the 4 key steps of food safety—clean, separate, cook, and chill (<https://www.foodsafety.gov/keep-food-safe/4-steps-to-food-safety>).

Q: Is the U.S. food supply safe?

A: Currently there is no evidence of food or food packaging being associated with transmission of COVID-19.

Unlike foodborne gastrointestinal (GI) viruses like norovirus and hepatitis A that often make people ill through contaminated food, SARS-CoV-2, which causes COVID-19, is a virus that causes respiratory illness and not gastrointestinal illness, and foodborne exposure to this virus is not known to be a route of transmission.

It may be possible that a person can get COVID-19 by touching a surface or object that has the virus on it and then touching their own mouth, nose, or possibly their eyes, but this is not thought to be the main way the virus spreads. It's always important to follow the 4 key steps of food safety—clean, separate, cook, and chill (<https://www.foodsafety.gov/keep-food-safe/4-steps-to-food-safety>).

Q: Is the U.S. animal food supply safe?

A: Currently there is no evidence of animal food or food packaging being associated with transmission of COVID-19.

Foodborne exposure to the virus that causes COVID-19 is not known to be a route of transmission.

Q: Can I get COVID-19 from a food worker handling my food?

A: Currently, there is no evidence of food or food packaging being associated with transmission of COVID-19. However, the virus that causes COVID-19 is spreading from person-to-person in some communities in the U.S. The CDC recommends that if you are sick, stay home until you are better and no longer pose a risk of infecting others.

Anyone handling, preparing and serving food should always follow safe food handling procedures (</food/buy-store-serve-safe-food/safe-food-handling>), such as washing hands and surfaces often.

Q: Should food workers who are ill stay home?

A: CDC recommends that employees who have symptoms of acute respiratory illness stay home and not come to work until they are free of fever (100.4° F [37.8° C] or greater using an oral thermometer), signs of a fever, and any other symptoms for at least 24 hours, without the use of fever-reducing or other symptom-altering medicines (e.g. cough suppressants). Employees should notify their supervisor and stay home if they are sick. We recommend that businesses review CDC's interim guidance for businesses and employers (<https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html>)

CDC_AA_refVal=<https://www.cdc.gov/coronavirus/2019-ncov/specific-groups/guidance-business-response.html>) for planning and responding to coronavirus disease. Also see the FDA's Retail Food Protection: Employee Health and Personal Hygiene Handbook (</food/retail-food-industryregulatory-assistance-training/retail-food-protection-employee-health-and-personal-hygiene-handbook>).

Q: Should food facilities (grocery stores, manufacturing facilities, restaurants, etc.) perform any special cleaning or sanitation procedures for COVID-19?

A: CDC recommends routine cleaning of all frequently touched surfaces in the workplace, such as workstations, countertops, and doorknobs. Use the cleaning agents that are usually used in these areas and follow the directions on the label. CDC does not recommend any additional disinfection beyond routine cleaning at this time.

View the current list of products that meet EPA's criteria for use against SARS-CoV-2 (<https://www.epa.gov/pesticide-registration/list-n-disinfectants-use-against-sars-cov-2>), the cause of COVID-19.

Restaurants and retail food establishments are regulated at the state and local level. State, local, and tribal regulators use the Food Code (</food/retail-food-protection/fda-food-code>) published by the FDA to develop or update their own food safety rules. Generally, FDA-regulated food manufacturers are required to maintain clean facilities, including, as appropriate, clean and sanitized food contact surfaces, and to have food safety plans in place. Food safety plans include a hazards analysis and risk-based preventive controls and include procedures for maintaining clean and sanitized facilities and food contact surfaces. See: FSMA Final Rule for Preventive Controls for Human Food (</food/food-safety-modernization-act-fsma/fsma-final-rule-preventive-controls-human-food>).

Q: What is the FDA doing to respond to foodborne illnesses during the COVID-19 pandemic?

A: The virus that causes COVID-19 is a virus that causes respiratory illness. Viruses like norovirus and hepatitis A that can make people sick through contaminated food usually cause gastrointestinal or stomach illness. Currently there is no evidence of food, food containers, or food packaging being associated with transmission of COVID-19.

The CDC, FDA, and USDA continue to work with state and local partners to investigate foodborne illness and outbreaks during the COVID-19 pandemic. The FDA's Coordinated Outbreak Response and Evaluation (CORE) Network manages outbreak response, as well as surveillance and post-response activities related to incidents involving multiple illnesses linked to FDA-regulated human food products. During this coronavirus outbreak, CORE's full-time staff will continue to operate to prepare for, coordinate and carry out response activities to incidents of foodborne illnesses.

The FDA's Center for Veterinary Medicine manages outbreak response for animal food and is similarly staffed and prepared to respond to incidents of foodborne illness in animals.

Animals, Pets and Animal Drug Products

Q: What is the FDA's role in regulating animal drugs, animal food (including pet food), and animal medical devices?

A: The FDA approves and regulates animal drugs to ensure they are safe and effective. In addition, the FDA helps ensure that animal food (including pet food) is safe and truthfully labeled. The FDA has post-market authority over veterinary medical devices.

Q: Can I give my pet COVID-19? Can I get COVID-19 from my pet or other animals?

A: There is a very small number of pets around the world reported to be infected with the virus that causes COVID-19 after having contact with a person with COVID-19. Based on the limited information currently available, the risk of animals spreading COVID-19 to people is considered low.

Until we learn more about how this virus affects animals, treat pets as you would other human family members to protect them from a potential infection.

- Do not let pets interact with people outside the household.
- Keep cats indoors when possible to prevent them from interacting with other animals or people.

- Walk dogs on a leash, maintaining at least 6 feet (2 meters) from other people.
- Avoid dog parks or public places where a large number of people gather.

Talk to your veterinarian if your pet gets sick or if you have any concerns about your pet's health. Learn more about Pet Safety & COVID-19 (</consumers/consumer-updates/helpful-questions-and-answers-about-coronavirus-covid-19-and-your-pets>).

Q: Is there a test for COVID-19 in pets? If so, has it been approved by the FDA?

A: Certain veterinary diagnostic laboratories have developed diagnostic tests for SARS-CoV-2, the virus that causes COVID-19, for use in pets if needed.

Diagnostic tests for animals are regulated differently than those for humans. The FDA does not require approval or clearance of a 510(k), PMA, or any other pre-market submission for devices, including diagnostic tests, intended for animal use. The FDA does, however, have post-market regulatory oversight over devices intended for animal use and can take appropriate regulatory action if an animal device is misbranded or adulterated.

Certain private, state, and university veterinary diagnostic laboratories have developed diagnostic tests for SARS-CoV-2, the virus that causes COVID-19, for use in dogs and cats. The FDA is also aware of at least two veterinary tests for COVID-19 in pets developed by commercial laboratories initially for internal surveillance, but the agency has not evaluated the validity of these tests. The tests are not currently available for routine testing. The decision to test pets should be made collaboratively between local, state, or federal public and animal health officials.



Q: Should I get my pet tested for COVID-19?

A: Routine testing of pets for COVID-19 is not recommended at this time. There is currently no evidence that animals are a source of COVID-19 infection in the United States. Based on the limited information available to date, the risk of pets spreading the virus is considered to be low. If your pet is sick, consult your veterinarian.

Animal testing is reserved for situations when (<https://www.cdc.gov/coronavirus/2019-ncov/php/animal-testing.html>) the results may affect the treatment or management of people and animals. If your veterinarian thinks your pet is a candidate for testing, they will consult the state veterinarian and public health officials. Do not contact your state veterinarians directly: they do not have the client/patient-veterinarian relationship that would allow them to fully understand the situation and they are also actively involved in other animal disease-related emergencies as well as response to COVID-19.

Q: What animal species can get COVID-19?

A: We currently don't fully understand how COVID-19 affects different animal species. We are aware of a very small number of pets, including dogs, cats and a ferret reported to be infected with the virus that causes COVID-19 after close contact with people with COVID-19.

Large cats in captivity, including several lions and tigers in a New York zoo (<https://newsroom.wcs.org/News-Releases/articleType/ArticleView/articleId/14084/Update-Bronx-Zoo-Tigers-and-Lions-Recovering-from-COVID-19.aspx>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>), a puma in South Africa, and tigers in a Tennessee zoo (https://www.zooknoxville.org/wp-content/uploads/2020/10/028-Zoo-Knoxville-Tiger-Tests-Positive-for-SARS-CoV-2-.pdf?_ga=2.16313462.1707933573.1604353641-1319189766.1604071942)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>) have tested positive for SARS-CoV-2, as have several gorillas at the San Diego zoo, after showing signs of respiratory illness. It is suspected these animals became sick after being exposed to zoo employees with COVID-19.

The virus that causes COVID-19 has been reported in minks on farms in the Netherlands, Denmark, Spain, Italy, Sweden and the United States. Once the virus is introduced on a farm, spread can occur between mink as well as from mink to other animals on the farm (dogs, cats). Because some workers on these farms had COVID-19, it is likely that infected farm workers were the initial source of mink infections.

Recent research shows that ferrets, cats, fruit bats, and golden Syrian hamsters can be experimentally infected with the virus and can spread the infection to other animals of the same species in laboratory settings. Mice, pigs, chickens, and ducks did not become infected or spread the infection based on results from these studies. Data from one study suggest that dogs are not as likely to become infected with the virus as cats and ferrets. These findings were based upon a small number of animals and do not indicate whether animals can spread infection to people.

For any animal that tests positive for SARS-CoV-2 at a private or state laboratory, USDA's National Veterinary Services Laboratories performs additional testing to confirm the infection and posts the results on this page: Cases of SARS-CoV-2 in Animals in the United States (https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/SA_One_Health/sars-cov-2-animals-us).

Q: Since domestic cats can get infected with the virus that causes COVID-19, should I worry about my cat?

A: We are still learning about this virus and how it spreads, but it appears it can spread from humans to animals in some situations. The FDA is aware of a very small number of pets, including cats, reported to be infected with the virus that causes COVID-19. The majority of these cases were linked to close contact with people who tested positive for COVID-19.

At this time, there is no evidence that pets, including cats and dogs, play a role in spreading COVID-19 to people. The virus that causes COVID-19 spreads mainly from person to person, typically through respiratory droplets from coughing, sneezing, or talking.

People sick with COVID-19 should isolate themselves from other people and animals, including pets, during their illness until we know more about how this virus affects animals. If you must care for your pet or be around animals while you are sick, wear a cloth face covering and wash your hands before and after you interact with pets.

Q: Why are animals being tested when many people can't get tested?

A: The FDA, USDA and CDC recommend that any testing of animals should be conducted using kits not required when testing people. USDA's National Veterinary Services Laboratories (NVSL) and the laboratories of the National Animal Health Laboratory Network (NAHLN) use tests developed for animal testing that are not used for testing in people. This avoids placing additional stresses on human testing resources while also recognizing the potential importance of animal testing to supporting public health.

Although animal and human tests are generally similar, this type of testing has to be adjusted in each species and for each sample type (blood, feces, nasal swab). Human and animal tests are not intended to be interchangeable. Some testing performed on animals is based on the published tests used in people, but animal testing is not likely to reduce the availability of tests for people if labs follow recommendations from the FDA, USDA, and CDC that animal testing be conducted using tests developed for animals.

Q: Can pets carry the virus that causes COVID-19 on their skin or fur?

A: Although we know certain bacteria and fungi can be carried on fur and hair, there is no evidence that viruses, including the virus that causes COVID-19, can spread to people from the skin, fur, or hair of pets.

However, because animals can sometimes carry other germs that can make people sick, it's always a good idea to practice healthy habits (<https://www.cdc.gov/healthypets/publications/stay-healthy-pets.html>) around pets and other animals, including washing hands before and after interacting with them and especially after cleaning up their waste.

There are no products that are FDA-approved to disinfect the hair or coats of pets, but if you do decide to bathe or wipe off your pet, first talk to your veterinarian about suitable products. Never use hand sanitizer, counter-cleaning wipes or other industrial or surface cleaners, as these can penetrate the skin or be licked off and ingested by your pet. If you have recently used any of these products on your pet, or your pet is showing signs of illness after use, contact your veterinarian and rinse or wipe down your pet with water.

Q: Are there any approved products that can prevent or treat COVID-19 in animals?

A: No. Under the Federal Food, Drug, and Cosmetic (FD&C) Act, “articles intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals” are drugs. The FDA has not approved any drugs for the diagnosis, cure, mitigation, treatment, or prevention of COVID-19 in animals. The U.S. Department of Agriculture’s (USDA) Animal and Plant Health Inspection Service (APHIS) Center for Veterinary Biologics (CVB) (<https://www.aphis.usda.gov/aphis/ourfocus/animalhealth/veterinary-biologics>) regulates veterinary biologics, including vaccines, diagnostic kits, and other products of biological origin. Similarly, APHIS CVB has not licensed any products to treat or prevent COVID-19 in animals.

The FDA has taken action against unapproved products claiming to prevent or cure COVID-19. The public can help safeguard human and animal health by reporting any products claiming to do so to FDA-COVID-19-Fraudulent-Products@fda.hhs.gov (<mailto:FDA-COVID-19-Fraudulent-Products@fda.hhs.gov>) or 1-888-INFO-FDA (1-888-463-6332).


Q: Is it true that animals, like dogs, cats, and cattle, get their own different types of coronavirus?

A: Yes. Coronaviruses are a large family of viruses. Some coronaviruses like COVID-19 cause cold-like illnesses in people, while others cause illness in certain types of animals, such as cattle, camels, and bats. Some coronaviruses, such as canine and feline coronaviruses, only infect animals and do not infect humans. For example, bovine coronavirus causes diarrhea in young calves, and pregnant cows are routinely vaccinated to

help prevent infection in calves. This vaccine is only licensed for use in cattle for bovine coronavirus and is not licensed to prevent COVID-19 in cattle or other species, including humans.

Dogs can get a respiratory coronavirus, which is part of the complex of viruses and bacteria associated with canine infectious respiratory disease, commonly known as “kennel cough.” While this virus is highly contagious among both domestic and wild dogs, it is not transmitted to other animal species or humans.

Most strains of feline enteric coronavirus, a gastrointestinal form, are fought off by a cat’s immune system without causing disease. However, in a small proportion of these cats, the virus can cause feline infectious peritonitis (FIP), a disease that is almost always fatal.

Other species, like horses, turkeys, chickens, and swine, can contract their own species-specific strains of coronavirus but, like the other strains mentioned above, they are not known to be transmissible to humans. More information is available in the American Veterinary Medical Association’s fact sheet about coronaviruses in domestic species (<https://www.avma.org/sites/default/files/2020-02/AVMA-Coronavirus-Taxonomy-Notes.pdf>)  (<http://www.fda.gov/about-fda/website-policies/website-disclaimer>).

Q: If my pet previously had a species-specific coronavirus, does that make them more or less likely to get COVID-19?

A: There are no data to suggest that current or previous infection with another strain of coronavirus would make your pet more or less likely to get COVID-19.

Q: If my pet has been vaccinated for species-specific coronavirus, does that make them more or less likely to get COVID-19?

A: Species-specific coronavirus vaccines are unlikely to work against this type of coronavirus because it is a new virus that is different from the species-specific strains of coronavirus targeted by the vaccine.

Q: My pet has health problems and goes to the vet regularly for treatment. Should I be doing anything different to manage their health during the COVID-19 outbreak?

A: While you should not avoid necessary visits to your veterinarian due to the COVID-19 outbreak, you should exercise reasonable caution just like you would if you were going to any other public place. If you are concerned about your own health or that of your pet when

going to the veterinarian, contact their office in advance to discuss any recommended precautions.

Q: Is it safe to adopt pets from a shelter or rescue?

A: There is no reason to think that any animals, including shelter or rescue pets, in the United States, might be a source of COVID-19. The virus that causes COVID-19 spreads mainly from person to person, typically through respiratory droplets from coughing, sneezing, or talking.

Q: Are there going to be any animal drug shortages due to the COVID-19 outbreak?

A: The FDA has been and is continuing to closely monitor how the COVID-19 outbreak may impact the animal medical product supply chain.

We have been reaching out to manufacturers as part of our approach to identifying potential disruptions or shortages. We will use all available tools to react swiftly to help mitigate the impact if a potential disruption or shortage is identified.

Learn more on our [Animal Drug Shortage Information](/animal-veterinary/product-safety-information/animal-drug-shortage-information) page (/animal-veterinary/product-safety-information/animal-drug-shortage-information).



Protect Yourself

AVOID COVID-19 Vaccine Scams

As COVID-19 vaccine distribution begins, here are signs of potential scams:

- You are asked to pay out of pocket to get the vaccine.
- You are asked to pay to put your name on a vaccine waiting list or to get early access.
- Advertisements for vaccines through social media platforms, email, telephone calls, online, or from unsolicited/unknown sources.
- Marketers offering to sell or ship doses of the vaccine for payment.
- ✓ **Protect Yourself. Do not give out your personal information to unknown sources.**

! If you believe you have been the victim of COVID-19 fraud, immediately report it to:

- HHS-OIG Hotline: **1-800-HHS-TIPS** | tips.hhs.gov
- FBI Hotline: **1-800-CALL-FBI** | ic3.gov
- CMS/Medicare Hotline: **1-800-MEDICARE**



For accurate, up-to-date information about COVID-19, visit:

oig.hhs.gov/coronavirus
fbi.gov/coronavirus
justice.gov/coronavirus



HHS
Office of
Inspector
General



Federal
Bureau of
Investigation



Department
of Justice

