Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Tabulating COVID-19-Related Fraud and Financial Loss

March 31, 2021

Fraudsters have leveraged the Coronavirus Disease 2019 (COVID-19) pandemic to take advantage of both individuals and organizations. Their schemes range from posing as representatives of a charitable organization or government agency and tricking individuals into providing money or personally identifiable information (PII), to selling bogus or counterfeit treatments or vaccines for COVID-19 or protective equipment and medical devices, that may or may not be delivered after victims submit payment. Scammers have also tried to use stolen PII to gain access to and steal unemployment benefits and economic impact payments provided pursuant to the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; P.L. 116-136) and other legislation aimed at providing COVID-19-related relief and recovery.

While the pandemic has created new opportunities for fraudsters, they still rely upon a number of tried-and-true tools to scam victims or gain access to information, accounts, and resources. For instance, they continue to make robocalls, phish for information through emails and social media, install malware on unsuspecting users' devices, and exploit technology vulnerabilities. In addition, criminals leverage both the surface web and dark web to facilitate these schemes.

In conducting oversight over federal law enforcement's efforts to investigate COVID-19-related fraud and the associated financial losses, policymakers may look to available data surrounding these scams to aid them with their work.

Reporting COVID-19 Scams

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

- **National Center for Disaster Fraud (NCDF).** The NCDF is a repository for the public to report complaints of disaster-related fraud to the Department of Justice (DOJ). It was created in the wake of Hurricane Katrina and continues to serve as a resource for

Congressional Research Service
https://crsreports.congress.gov
IN11640

reporting fraud related to natural and man-made disasters. DOJ has directed the public to report COVID-19-related scams to the NCDF.

- **Internet Crime Complaint Center (IC3).** The IC3 is a mechanism for the public to report all types of internet-related crime to the Federal Bureau of Investigation (FBI). Originally established as the Internet Fraud Complaint Center in 2000, it was renamed in 2003 to reflect the nature of the internet- and cyber-related crimes reported to the center. In addition to providing information to law enforcement, the IC3 also shares alerts with industry partners and the public.
- **Consumer Sentinel.** The Federal Trade Commission's (FTC's) Consumer Sentinel is a mechanism for the public to report a range of consumer complaints to the commission, which in turn shares these complaints with federal, state, and local law enforcement. The Sentinel network provides law enforcement with tips on complaints, including fraud involving consumer product scams, credit and telemarketing scams, and identity theft.
- **FBI's tip line.** The FBI accepts tips on potential terrorist activity and reports of federal crimes such as fraud—including COVID-19-related fraud. However, callers are directed to report internet-based fraud to the IC3. (Other federal, state, and local law enforcement entities have their own tip lines where individuals can report scams.)

Data on COVID-19-Related Scams

While there is no central repository for reports on COVID-19-related fraud, two of the entities discussed above have published data that help provide snapshots of the nature and extent of this fraud.

- **Internet Crime Complaint Center Data.** The IC3 received 791,790 complaints in 2020 (a 69% increase over the 467,361 complaints received in 2019), involving more than $4.1 billion in reported losses. Approximately 28,500 of the complaints submitted to the IC3 in 2020 were related to COVID-19. Major categories of complaints related to COVID-19 include targeting CARES Act funds, particularly Unemployment Insurance, Paycheck Protection Program loans, and Small Business Economic Injury Disaster loans; impersonating government officials and attempting to solicit money or gain personal information; and, more recently, exploiting public interest in a vaccine to scam individuals out of money and information. The IC3 did not report on money lost specifically to COVID-19-related fraud.
- **Consumer Sentinel Data.** The FTC provides daily updates regarding Consumer Sentinel complaints related to COVID-19. Between January 1, 2020, and March 28, 2021, the FTC received 411,661 such complaints, including 226,023 reports of fraud. Of these fraud complaints, 42% reported financial loss, and these reported losses totaled $386.8 million. The fraud categories with the most COVID-19-related reports have been online shopping (e.g., unreceived goods complaints) and vacation and travel (e.g., refund and cancellation complaints).

Data Gaps

These data presented by the IC3 and FTC present snapshots of fraud, as reported by potential victims. Notably, these self-reported data may not reflect losses to all individuals, as data are dependent upon factors including the recognition that victimization has occurred and an individual's choice of if, when, or where to report (and research indicates that many crime victims do not report their victimization to law enforcement). In addition, reported victims of fraud in these instances are individuals, not organizations or government programs. There are a number of programs that have reportedly fallen victim to fraud, including unemployment benefits, small business grants and loans, and

economic impact payments pursuant to the CARES Act and other relief packages. DOJ, through press releases about arrests and prosecutions of individuals suspected of defrauding these programs, provides examples of these scams and losses associated with specific cases. However, total program losses from fraud are not included in the data presented by the FBI and FTC, thus limiting information about the extent and financial effects of COVID-19-related fraud. Notably, the Internal Revenue Service, DOJ, FTC, and other entities have cautioned about further economic impact payment scams that will likely be associated with the American Rescue Plan Act of 2021 (P.L. 117-2).

Author Information

Kristin Finklea
Specialist in Domestic Security

Disclaimer