Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

# COVID-19 and Emerging Global Patterns of Financial Crime

September 4, 2020

Criminal groups around the world are exploiting opportunities for illicit profit during the COVID-19 pandemic. As criminal behaviors shift, so, too, have the illicit financial footprints left behind. As Congress considers U.S. and international responses to the pandemic, it may also examine the emerging risks and financial patterns associated with COVID-19-related criminal activity, including cybercrime.

## Risk Context

According to the Financial Action Task Force (FATF), an intergovernmental standards-setting body on anti-money laundering (AML) and counter-financing of terrorism (CFT), as well as other reporting, the pandemic has contributed to significant changes in the financial behavior of governments, businesses, and people in many parts of the world. These changes have also introduced new money laundering and financial fraud risks. For example:

- Economic uncertainty, characterized by high unemployment, business insolvency, and disruptions in global trade patterns, has mobilized governments around the world to introduce large-scale emergency financial assistance and stimulus programs. Increased availability of government funds may challenge authorities to identify fraudulent claims, as well as misappropriated and misdirected funds due to corruption.
- Voluntary and government-mandated quarantines and stay-at-home orders have reduced in-person banking activity and increased online banking and remote transactions. This increase in remote banking has challenged financial institutions to comply with AML/CFT requirements related to customer identity verification and due diligence.
- Financial volatility has driven investors to redistribute assets, resulting in liquidated portfolios, large funds transfers, and increases in physical cash holdings, safe haven assets (e.g., gold), real estate purchases, and virtual currencies. Major changes in financial transaction patterns may obscure criminal activity, particularly when assets are converted into less transparent and less traceable forms.
- Public health concerns have resulted in the postponement of some on-site inspections of financial institutions, delays in some reporting of suspicious financial activity and

**Congressional Research Service**
https://crsreports.congress.gov
IN11496

transactions, and, in some countries, a reprioritization of scarce government resources away from AML/CFT.

## Illicit Finance Patterns

While disruptions in the movement of people and goods during the pandemic appear to have reduced certain types of financial crime, including cash-courier and trade-based money laundering, the pandemic has increased the vulnerability of certain individuals to COVID-19-related criminal schemes. The primary financial crime risks associated with the COVID-19 crisis involve the laundering of illicit proceeds, particularly fraud. Opportunities for perpetrating cyber-enabled crimes have also increased.

### Fraud

The COVID-19 pandemic has exacerbated fraud, which remains at the forefront of money laundering concerns, both domestically and abroad. Even prior to the pandemic, the 2018 U.S. National Money Laundering Risk Assessment reported that fraud represented the crime that generates the most illicit proceeds in the United States. Common forms of pandemic fraud include medical-related products fraud (e.g., nondelivery fraud, price gouging and hoarding, as well as the sale of counterfeit, substandard, unapproved, and misbranded products), securities fraud (e.g., insider trading, investment scams, and retirement account fraud), and imposter scams (e.g., charities fraud and "faking-and-entering" schemes). Amid the COVID-19 crisis, according to the European Police Organization (EUROPOL), counterfeit surgical masks represent the most commonly sold medical product online. The International Criminal Police Organization (INTERPOL) has issued a Purple Notice on COVID-19 fraud schemes involving transnational financial payment patterns.

### Exploitation

The pandemic has created opportunities for criminals to target certain populations, particularly those who are economically insecure or exploitable, while engaging in online transactions and activities (e.g., the elderly and children). Based on financial institution reporting, the Financial Crime Enforcement Network (FinCEN) has highlighted the prevalence of money mule schemes during the pandemic; in such schemes, criminals recruit witting and unwitting individuals to transfer illegally acquired money on their behalf. Several recent reports have emphasized the pandemic's potential to isolate victims of domestic servitude, endanger victims of sex trafficking, and provide online sex offenders with more opportunities to target children. Pandemic-related border control measures are also causing asylum seekers, refugees, and migrants, many of whom may be undocumented, to take more dangerous smuggling routes.

### Cybercrime

More online activity during the pandemic has resulted in more opportunities for cybercriminals to target individuals and businesses. Greater dependence on remote and virtual platforms during the pandemic has further exposed cyber vulnerabilities, including those of financial and health care systems. Cybercriminals are repurposing known schemes (e.g., phishing campaigns, malware distribution, and business email compromise schemes) to target victims with COVID-19-related lures. FinCEN reports that cybercrime money laundering primarily involves virtual currency. According to INTERPOL, there has been an increase in malicious and high-risk domains registered with COVID-related keywords. EUROPOL has further reported an intensification of cyberattacks during the pandemic and a shorter period between an initial ransomware infection and activation of the attack, as well as ongoing use of dark web platforms to distribute illicit goods and services.

## Outlook

While some of the short-term manifestations of COVID-19-related criminality are emerging, the longer-term implications remain unclear. Some observers posit that the pandemic may be creating new classes of criminals and victims that could have lasting repercussions for transnational crime. Moreover, the total financial scale, global impact, and consequences of COVID-19-related crimes may remain unknown for years, including corruption schemes and the true scope of illicit actors involved (which may include state actors, drug traffickers, and terrorists). In the meantime, policy responses to the financial crime risks associated with the pandemic have included public awareness campaigns, collection and analysis of financial intelligence, and ongoing law enforcement activity. A key issue on the horizon for policymakers is to anticipate how criminals will exploit the post-pandemic environment.

As Congress continues to consider various aspects of the international pandemic policy response, oversight from a financial crime perspective may focus on whether the existing AML/CFT policy framework, risk assessments, and strategy are sufficient to meet pandemic-related challenges. It may also consider how proposed legislative changes to the existing AML/CFT regime, if enacted, could contribute (or not) to addressing COVID-19-related illicit finance. Currently pending in the 116th Congress is the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (H.R. 6395), which incorporated several AML/CFT reform proposals, including the Corporate Transparency Act of 2019 (H.R. 2513) and the COUNTER Act of 2019 (H.R. 2514), as well as the ILLICIT CASH Act (S. 2563).

## Author Information

Liana W. Rosen
Specialist in International Crime and Narcotics

## Disclaimer