FACTCOALITION
Financial Accountability & Corporate Transparency

June 16, 2020

The Honorable Emanuel Cleaver
Chairman
Subcommittee on National Security, International Development, and Monetary Policy
U.S. House of Representatives Committee on Financial Services
Washington, DC 20515

The Honorable French Hill
Ranking Member
Subcommittee on National Security, International Development, and Monetary Policy
U.S. House of Representatives Committee on Financial Services
Washington, DC 20515

RE: Virtual Hearing titled "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic"

Dear Chairman Cleaver and Ranking Member Hill,

On behalf of the Financial Accountability and Corporate Transparency (FACT) Coalition, we appreciate the opportunity to comment on your hearing titled, "Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic." The FACT Coalition is a non-partisan alliance of more than 100 state, national, and international organizations promoting policies to combat the harmful impacts of corrupt financial practices.[1]

Financial crime is large and has been growing at a startling rate for years. Prior to the onset of the pandemic, the International Monetary Fund (IMF) and United Nations Office on Drugs and Crime (UNODC) estimate the scale of global money laundering falls somewhere around two to five percent of global gross domestic product — or approximately $1.7 trillion to $4.3 trillion in 2018.[2] Alarmingly, UNODC estimates that less than 1 percent of these illicit financial flows are seized and forfeited — thus perpetuating and rewarding transnational criminal activities from drug dealing and human trafficking to cybercrime and the illicit trade in counterfeit and pirated goods.[3]

For nearly a decade, the FACT Coalition and our members have warned about the alarming scale of international money laundering and its corrosive impacts on our society. For years, the world has faced a pandemic of financial crime, cybercrime, and corruption. The new COVID-19

[1] A full list of FACT members is available at http://thefactcoalition.org/about/coalition-members-and-supporters/.
[2] UN Office on Drugs and Crime (UNODC), "Money Laundering and Globalization," Accessed June 15, 2020, https://www.unodc.org/unodc/en/money-laundering/globalization.html.
[3] UN Office on Drugs and Crime (UNODC), "UNODC Estimates that Criminals May Have Laundered US$ 1.6 Trillion in 2009," https://www.unodc.org/unodc/en/press/releases/2011/October/unodc-estimates-that-criminals-may-have-laundered-usdollar-1.6-trillion-in-2009.html.

pandemic has generated an unparalleled global health and economic crisis, which — left unaddressed — will only exacerbate such illicit activity.

Illicit Trade

The Organization for Economic Cooperation and Development (OECD) and European Union Intellectual Property Office (EU IPO) estimate that the value of imported counterfeit goods worldwide was US$509 billion in 2016, amounting to 3.3 percent of world trade. While this illicit trade costs businesses an enormous amount of money in lost revenues and reputational harm, counterfeit products can pose serious health and safety risks to consumers and communities. The U.S. Departments of Homeland Security and Justice, as well as INTERPOL, have recently noted that criminals are taking advantage of the COVID-19 crisis by hawking counterfeit cleaning disinfectants, medicines, medical supplies and equipment, and other goods — including through the use of online marketplaces, the darkweb, and social media.[4]

In one startling example, more than 1,300 Chinese companies supplying medical equipment to the U.S. to fight COVID-19 used as their U.S. agent for FDA registration a purported Delaware company with false address and nonworking phone number, thereby circumventing additional regulatory oversight. [5]

Cybercrime

In May, the United Nations Under-Secretary-General of Disarmament Affairs warned that global cybercrime is increasing during the COVID-19 pandemic, with a 600 percent jump in malicious emails being sent; cyberattacks now happen once every 39 seconds.[6] This was echoed by your witness, Tom Kellermann, at the Financial Services Committee roundtable last month. He noted that there was a 238 percent increase on targeted cyberattacks on the U.S. financial sector from February through April 2020, while ransomware attacks on hospitals and medical facilities have seen a 900 percent increase during the pandemic.[7] The financial implications of

[4] *U.S. Department of Homeland Security*, OPERATION STOLEN PROMISE, "An Initiative Targeting COVID-19 Fraud", Homeland Security Investigations, May 2020, https://www.ice.gov/topics/operation-stolen-promise; *U.S. Department of Justice*, "Justice Department Files Its First Enforcement Action Against COVID-19 Fraud", March 22, 2020, https://www.justice.gov/opa/pr/justice-department-files-its-first-enforcement-action-against-covid-19-fraud; *INTERPOL*, "Coronavirus outbreak sparks a new trend in counterfeit medical items: Criminals are cashing in on COVID-19", March 19, 2020, https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19.

[5] Austen Hufford, Mark Maremont and Liza Lin, "Over 1,300 Chinese Medical Suppliers to U.S.—Including Mask Providers—Use Bogus Registration Data," *Wall Street Journal*, June 12, 2020, https://www.wsj.com/articles/over-1-300-chinese-medical-suppliers-to-u-s-including-mask-providersuse-bogus-registration-data-11591991270?shareToken=st497a9f091e784abc9388e22c05c38230.

[6] Edith Lederer, "Top UN Official Warns Malicious Emails on Rise in Pandemic," *AP NEWS*, Associated Press, May 23, 2020, apnews.com/c7e7fc7e582351f8f55293d0bf21d7fb.

[7] Tom Kellermann, Written Testimony before the House Financial Services, National Security, International Development, and Monetary Policy Subcommittee, May 28, 2020, https://financialservices.house.gov/uploadedfiles/kellermann_statement_to_congressional_roundtable.pdf; Jericho Casper, "Increased Telework on Broadband Networks Leads to Surge in Cybersecurity Vulnerabilities," Broadband and Breakfast, May

this are astounding. Even before the pandemic, a recent report by Cybersecurity Ventures estimated that the global financial costs from cybercrime would double from US$3 trillion in 2015 to US$6 trillion by 2021.[8]

Anti-money laundering experts have warned that anonymous shell corporations are one of the primary tools through which cybercriminals move their funds. [9]

In addition to criminals seeking financial gain, U.S. adversaries are similarly exploiting these cyber-vulnerabilities. According to the Federal Bureau of Investigation, Chinese hackers are launching cyberattacks on U.S. research organizations to steal information on vaccines, treatments, and testing.[10]

Corruption

At the same time, UNODC has estimated that up to 25 percent of government procurement is lost to corruption each year — wasting taxpayer money, hollowing out public services, and raising direct national security concerns as our adversaries enrich themselves through graft.[11] As governments around the world enact major stimulus plans, anticorruption and transparency measures must be a priority.

At $2.7 trillion, the recently-enacted CARES Act and subsequent Paycheck Protection Program and Health Care Enhancement Act amount to the largest economic stimulus response in U.S. history, while lawmakers are already working on additional measures. While certainly warranted, the rapid disbursement of capital on such a large scale does present an enormous risk for waste, fraud, abuse, and corruption — making it all the more alarming that the bills contained minimal oversight, transparency, and accountability measures.

Recommendations

It is more important than ever that we strengthen our anti-money laundering safeguards.

28, 2020, http://broadbandbreakfast.com/2020/05/increased-telework-on-home-broadband-networks-leads-to-surge-in-cybersecurity-vulnerabilities.

[8] "Cybercrime Damages $6 Trillion by 2021," Cybersecurity Ventures, October 16, 2017, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

[9] John Bandler, Esq., CAMS, "Stemming the Flow of Cybercrime Payments," *ACAMS Today*, JUNE 9, 2017, https://www.acamstoday.org/stemming-the-flow-of-cybercrime-payments/.

[10] *Federal Bureau of Investigation,* "People's Republic of China Targeting of COVID-19 Research Organizations," May 13, 2020, https://www.fbi.gov/news/pressrel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations.

[11] UN Office on Drugs and Crime (UNODC), "Good Practices in Ensuring Compliance with Article 9 of United Nations Convention against Corruption," p. 1, September, 2013, https://www.unodc.org/documents/corruption/Publications/2013/Guidebook_on_anti-corruption_in_public_procurement_and_the_management_of_public_finances.pdf

One essential, commonsense way to ensure the integrity of our COVID-19 response and crackdown on cybercrime, fraud, and other illicit behavior is to end the incorporation of anonymous companies in the United States. Opaque corporate entities are a key tool used by cybercriminals, fraudsters, purveyors of counterfeit and pirated goods, and corrupt actors to launder their proceeds and mask their identities from law enforcement. A 2014 study found that, among the 103 countries they studied, the United States is the easiest place for suspicious individuals to incorporate an anonymous company.[12]

The House of Representatives — led by this Committee — took the lead last year in passing the bipartisan Corporate Transparency Act of 2019 (H.R. 2513) to shine a light on the true owners of corporate entities formed in the U.S. Unfortunately, despite widespread support from the national security, law enforcement, human rights, and anticorruption communities, the Senate has thus far failed to move forward on its companion legislation, known as the ILLICIT CASH Act (S.2563). Such inaction leaves the American people vulnerable to the cybercrime, fraud, and corrupt activity that is facilitated by anonymous companies during the pandemic. It's time for the Senate to seize this once-in-a-generation opportunity to enact a key structural reform to protect our communities from financial abuse in this difficult time.

Thank you very much for considering the Coalition's thoughts on this topic. Should you have any questions, please feel free to contact Erica Hanichak at ehanichak@thefactcoalition.org.

Sincerely,

Clark Gascoigne
Interim Executive Director

Erica Hanichak
Government Affairs Director

[12] Michael Findley, *Global Shell Games: Experiments in Transnational Relations, Crime, and Terrorism*, p. 74, January 2014, https://bit.ly/2uTLptQ.