

# **MICHIGAN STATE UNIVERSITY**

Select Subcommittee Office  
2157 Rayburn House Office Building  
Washington, D.C. 20515  
ATTN: Rep. James E. Clyburn, Chairman

December 15, 2021

RE: Response to Post-Hearing Questions

Chairman Clyburn,

Thank you for inviting me to testify before the House Select Subcommittee on the Coronavirus Crisis on November 17<sup>th</sup> of this year. Addressing the many threats facing American consumers as fraudsters attempt to take advantage of the pandemic is an important and worthy battle needing to be fought. The following are my responses to the questions posed by Rep. Bill Foster following the hearing. They reflect my research on frauds and crime generally, my specific work on COVID-19 frauds, and my experiences investigating white-collar crimes. Where I have offered opinions they are solely my own and do not reflect the university or my colleagues positions.

- 1. How are fraudsters using the coronavirus to prey on consumers, and what are some of the ways communities of color are specifically targeted by online misinformation and virus-related schemes?*

During the pandemic COVID-19 fraudsters have used a number of Internet-based schemes to reach consumers. Given lockdowns and the significant increases in use of the Internet to obtain news, information, and goods and services, this is not surprising. Also, the Internet affords fraudsters a wide degree of autonomy and invisibility. In our research, we found that more than 42% of respondents believed they had been targeted by fraudsters pushing a COVID-19 related product or service. Many of these frauds were designed to steal consumers information or money, as nearly 35% of people who purchased a product or service never received what they had paid for. Of those individuals who did receive their purchase, 84% later found out that it was not genuine.

Americans who were victimized by COVID fraudsters were significantly more likely to be younger and Black/African American, and significantly less likely to be White or Asian. Americans who were unemployed due to the pandemic were significantly more likely to believe they were being targeted by fraudsters. These findings further reinforce the fact that fraudsters have been targeting those most affected by the pandemic. We also found that the targets of COVID-19 frauds spent more time online (about an hour more, on average) than those who were not targeted for fraud.

Victims of COVID-19 frauds reporting spending an average of \$444.44 on COVID-related expenses, and many were able to recover their funds once they found out they had been deceived as many people used credit or debit cards to make their purchases. We do not know the specific ways in which communities



**College of  
Social Science**

School of Criminal  
Justice

Baker Hall  
655 Auditorium Road  
Room 557  
East Lansing, MI 48824

517-355-2197  
Fax: 517-432-1787  
cj.msu.edu

of color are targeted by fraudsters, but given that COVID-19 frauds follow the general patterns laid down by other fraud schemes it is reasonable to assume that targeted advertising through social media channels is the primary method. Additionally, the use of influencers is likely key to many schemes.

- 2. Have you seen evidence that some medical professionals or doctors' groups, like America's Frontline Doctors and SpeakWithAnMD.com, are incentivized to prescribe drugs like ivermectin and hydroxychloroquine to patients for financial gain?*

There are two answers to this question, both of which are equally valid: First, I have not seen evidence that covert actors, hidden parties, or some other unseen entity is providing a financial incentive to the individuals behind the sites mentioned for prescribing ivermectin or hydroxychloroquine. This would be very difficult to detect and likely would not come to light without some sort of law enforcement investigation into groups like America's Frontline Doctors, which would be able to turn up flows of funds to the group from nefarious sources.

Second, the incentive of financial gain is what is driving groups like this to provide for-fee services to individuals looking to obtain these treatments. Two sites in particular, America's Frontline Doctors, and FrontlineMDs operate much like fraudulent online healthcare sites. Specifically, they operate multiple sites with different, yet similar, domain names that provide overlapping yet distinct information. The financial gains realized by America's Frontline Doctors comes from observable and unobservable sources. The observable sources are provider fees (\$90 per telehealth consultation), which are made clear on their website. The unobservable are likely finder's fees that are paid to the website operators by their partners, which include firms like Gold Care Health and Wellness (<https://goldcaretelemed.com/>), Accurate Specialty Pharmacy (<https://arxspecialtypharmacy.com/>), and COVIDRX (no website identified). FrontlineMDs.com operates under a number of different site names, including the following: [frontlinemedicaldoctors.com](http://frontlinemedicaldoctors.com), [frontlinemds.com](http://frontlinemds.com), and [drstellamd.com](http://drstellamd.com).

Under this model, the site operators present themselves as healthcare professionals offering direct treatments to consumers. FrontlineMDs.com offers supplements labeled "COVILyte", "COVISpray" and "COVISleep", which are intended to treat or prevent COVID-19 and provide additional benefits such as general immune support, brain and energy support, address sleeplessness and other issues. In short, the revenue earned from prescribing ivermectin and hydroxychloroquine is itself the financial incentive necessary for fraudsters and other bad actors to initiate and continue their schemes.

- 3. Based on your research and expertise, what more can be done to combat online misinformation and protect vulnerable communities from virus-related fraud schemes?*

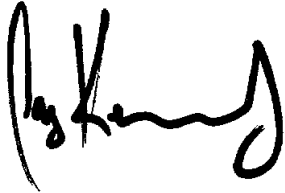
Unfortunately, there is no easy remedy to this issue, yet a multi-pronged approach may be helpful in combatting the proliferation of harmful misinformation and frauds, particularly within vulnerable communities. First, the politicization of masks, vaccines, and the effectiveness of treatments and other ways to respond to the coronavirus has created an informational war wherein messaging can be labeled illegitimate, misleading, or fraudulent simply because of its source. This is particularly the case with official messaging coming from the federal government when such messaging is contradicted by legitimate-appearing sources. For example, the coverage of a French Nobel prize winning doctor's anti-vaccination statements have been picked up by *The New American*, an online outlet that opposes the vaccine and vaccine mandates. This outlet used the Nobel prize winner's statement as a legitimate counterargument to narratives encouraging Americans to become vaccinated. Other sources make very compelling and legitimate-appearing statements intended to erode confidence in official narratives and federal agencies.

Given the spread of these types of messaging it is essential that the definition of "vulnerable" communities be expanded to include not only the economically and socially marginalized (including those who are at elevated risk for financial victimization) but also the communities that are most susceptible to buying-in to messages that dispute legitimate, official information. Finding a way to de-politicize messaging and information about the virus, the vaccine and related issues should be a primary goal. Skeptics have latched on to official counts of COVID-19 deaths looking for avenues to attack the legitimacy of the numbers, which they then use to discredit the sources of those numbers. Discrediting those sources leads to a delegitimization of the source.

Second, Congress should push the Biden Administration to nominate, and the Senate to confirm, a candidate for the role of Intellectual Property Enforcement Coordinator (IPEC), a cabinet position that has been vacant since the end of the Trump Administration. The IPEC can work within the US and across the globe to partner with other countries on stopping transnational groups from targeting and victimizing Americans in ways that infringe upon American intellectual property. This can include the sale of counterfeit, falsified and substandard drugs that are protected by US intellectual property protections, as well as the unauthorized use of logos and trademarks that are used to deceive consumers into believing that a site is legitimate. Furthermore, the IPEC can serve a key role in coordinating with public and private entities to address this problem on multiple fronts. Working with corporations, law enforcement, and online intermediaries the IPEC would be in an ideal position to affect online and offline COVID-19 frauds that involve the violation of intellectual property rights. Importantly, this work would have lasting impacts for the country, as the lessons learned and partnerships established would be effective in combatting intellectual property crimes generally, as well as those that are likely to develop during future pandemics or natural disasters.

Again, I thank you for the opportunity to testify and to provide responses to these important questions. If I can be of service to the Select Subcommittee in the future please do not hesitate to reach out.

Sincerely,

A handwritten signature in black ink, appearing to read "Jay Kennedy". The signature is stylized with a large initial "J" and a long, sweeping underline.

Jay P. Kennedy, Ph.D.  
Assistant Professor, School of Criminal Justice  
Assistant Director of Research, Center for Anti-Counterfeiting and Product  
Protection