U.S. House of Representatives
Select Subcommittee on the Coronavirus Crisis

Hearing on Combating Coronavirus Cons and the Monetization of Misinformation

November 17th, 2021

Written Statement
Submitted by:
Jay P. Kennedy, Ph.D.
Assistant Professor of Criminal Justice
Assistant Director of Research, Center for Anti-Counterfeiting and Product Protection
Michigan State University

Chairman Clyburn, Ranking Member Scalise and Members of the Select Subcommittee, good afternoon and thank you for inviting me to testify today. I appreciate your focus on the ongoing issues posed by COVID-19 related frauds, which continue to threaten the health and safety of American citizens. While I will make reference to, and draw upon, recent research exploring these frauds generally, as well as work that has been undertaken by the Center for Anti-Counterfeiting and Product Protection, the views that I express to you today are my own. These views are drawn from the research and outreach I have conducted in my role as an Assistant Professor of Criminal Justice at Michigan State University, and as the Assistant Director of Research for the Center for Anti-Counterfeiting and Product Protection. The Center for Anti-Counterfeiting and Product Protection, otherwise known as the A-CAPP Center, is a hub for interdisciplinary research, education and outreach within the brand protection community. Our mission is to engage with brand owners, law enforcement agencies, service providers, intermediaries, researchers and others to identify novel and effective solutions to the product counterfeiting challenges that face an increasingly connected global marketplace.

My research for the past decade has focused on both corporate crime and crimes committed against businesses, with a recent focus on counterfeit products, occupational frauds and insider threats, as well as the nature and structure of online frauds and counterfeiting schemes. My comments today reflect what colleagues and I have discovered regarding the nature and structure of COVID-19 frauds, as well as what we at the A-CAPP Center have identified regarding product counterfeiting during the pandemic. Through this testimony I hope to draw attention to four important issues, which I believe deserve continued awareness as they are vital to the protection of consumers. The first is the need to expand activities that proactively identify and disrupt opportunities for virus-related frauds. The second is the value of enhancing public-

private partnerships that support collaborative crime prevention strategies. The third is the substantial impact of misinformation and disinformation that continues to shape the nature and structure of pandemic-driven frauds. And finally, I will highlight the need to engage with the most vulnerable consumers as a way to help mitigate their exposure to fraud risks.

COVID-19 and Opportunities for Crime

It has been nearly two years since COVID-19 was declared a public health emergency by the U.S. government and the World Health Organization. Beyond the severe public health risks posed by the virus, it became clear from an early stage that criminals would take every opportunity to exploit the virus in pursuit of illicit gains. From the very beginnings of the pandemic, a mix of disinformation and misinformation, a lack of access to scientific data and information, and a general fear of the unknown combined to create an opportune environment for frauds to proliferate.

The research my colleagues and I undertook came early into the pandemic because we knew that it was not a question of if, but rather a question of when and how COVID-related frauds would appear. Part of our initial thinking around the spread of frauds came from an understanding that certain crimes tend to proliferate following natural disasters due to break downs in formal control.[1] Natural disasters also give rise to a large number of fraud schemes that are typically tied to rebuilding efforts and the distribution of economic resources and social assistance intended to benefit affected citizens.[2] Yet, as stated in our research on COVID-19

[1] Cromwell, P., Dunham, R., Akers, R., & Lanza-Kaduce, L. (1995). Routine activities and social control in the aftermath of a natural catastrophe. *European Journal on Criminal Policy and Research*, *3*(3), 56-69.
[2] Davila, M., Marquart, J. W., & Mullings, J. L. (2005). Beyond mother nature: Contractor fraud in the wake of natural disasters. *Deviant Behavior*, *26*(3), 271-293.

frauds[3], "unlike a hurricane, wildfire, or other natural disaster that has localized impacts on a particular subset of the population, COVID-19 is truly a global crisis, making the pool of potential victims much bigger." As the pool of potential victims grows, so to does the incentive for criminals to find ways to extract illicit gains by exploiting the crisis for their desired ends. Part of this exploitation rests upon an expectation that it will be relatively easy to find suitable targets who are relatively poorly guarded, and therefore incredibly suitable for victimization.

The COVID-related fraud opportunities that we have witnessed are the result of situations that allow criminal actors to interact with consumers within spaces that are poorly guarded and facilitate the hiding of criminal activity.[4] Disrupting these opportunities requires that criminals be prevented from reaching potential victims, that potential victims be appropriately guarded against victimization, or that the places – virtual or physical – wherein victims and offenders interact are better managed. Generally, fraud schemes are successful because the elements of the scheme remain relatively stable, which allows victimization to continue for long periods of time. However, we have seen COVID-19 fraud schemes shift rapidly in the past two years, and it was always clear from the beginning that the frauds we would see would change over the course of the pandemic.

While efforts to prevent the spread of these frauds have been active since the first weeks of the pandemic, criminals have adapted their behaviors as a response to crime prevention efforts. Consumers' vulnerability to these frauds is tied to the copious amounts of misinformation about the virus, as well as competing narratives about treatments and preventative medicines, which are prevalent throughout society. With each new narrative that

[3] Kennedy, J. P., Rorie, M., & Benson, M. L. (2021). COVID-19 frauds: An exploratory study of victimization during a global crisis. *Criminology & Public Policy*.
[4] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

develops, and as existing narratives continue to be propagated, opportunities for fraud and illicit criminal gain expand.

Public-Private Partnerships to Protect Consumers

The spread of misinformation during the pandemic, particularly that which has supported many fraud schemes, has primarily occurred online through social media platforms and to a lesser extent email. The ubiquity of the Internet and our cultural reliance upon the Internet for news and information has been both a blessing and a curse as it has allowed legitimate messaging to flow more quickly to larger numbers of people, while at the same time allowing for alternative messaging to develop and propagate. Misinformation and disinformation is spread through legitimate communication channels and fraudulent activities are often found on legitimate Internet sites. Effectively addressing these issues requires collaborations between public and private partners that involve information sharing and the exchange of data, as well as joint investigations.

One of the most prominent criminal schemes undertaken during the pandemic has been the wide distribution of counterfeit personal protective equipment (PPE), which began to enter the country soon after the introduction of counterfeit testing kits in March of 2020. These schemes have been the most persistent as criminals have sought to defraud consumers, healthcare facilities and governments by selling poorly made, ineffective counterfeit goods with reckless abandon. Highlighting the scale of this problem, in early 2021 federal authorities seized more than 18 million counterfeit N95 masks.[5] While the sheer scale of counterfeit PPE entering the country is staggering, this issue has drawn attention to the value of public-private partnerships

[5] https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-counterfeit-n95-masks

aimed at fighting criminal enterprises. The collaboration of U.S. law enforcement agencies with companies like 3M is admirable and must be highlighted as a model for effective anti-counterfeiting and crime prevention partnerships that need to continue, and deserve to be supported by federal, state and local agencies.[6] [7]

Public-private partnerships are essential to creating the information gathering and data sharing arrangements that allow for the development of effective anti-crime strategies. The Department of Homeland Security's National Intellectual Property Rights Coordination Center's collaborative efforts are an example of partnerships that can effectively identify and strategically address COVID-related fraud risks.[8] Working through a coordinating center, such as the National IPR Center or the Department of Justice's National Center for Disaster Fraud, allows for ongoing engagements that are built around the accomplishment of tangible fraud prevention goals.

The Challenges of Dealing with Misinformation

Unlike previous global pandemics, the ubiquity of the Internet and reliance upon the Internet for news and information, sometimes from unverified or less than legitimate sources, has helped to propagate misinformation about the virus. Unsurprisingly, the Internet has been a primary tool of fraudsters during the pandemic.[9] Beyond the issue of frauds, the spread of misinformation has been a continual challenge over the course of the pandemic, placing lives at risk and threatening to further exacerbate the social harms attributable to the virus. Our work in the area of counterfeit products has shown how easy it is for social media influencers, as well as general social media users, to impact perceptions about deviant behavior and shape narratives in

[6] https://www.3m.com/3M/en_US/worker-health-safety-us/covid19/covid-fraud/
[7] https://www.cbp.gov/newsroom/local-media-release/108000-counterfeit-3m-surgical-masks-stopped-cincinnati-cbp
[8] https://www.ice.gov/news/releases/hsi-partners-warn-consumers-covid-19-post-vaccine-survey-scam
[9] Levi, M., & Smith, R. G. (2021). Fraud and pandemics. *Journal of Financial Crime*.

such a way that facts, reason and evidence that disconfirms their opinion is perceived by their followers as illegitimate or baseless.[10]

While several federal agencies have been active in their attempts to spread legitimate information about the coronavirus, they have likely come to realize that it is much more difficult to influence consumer decision-making than it is to simply raise awareness about risky behaviors. Even before the pandemic, consumers regularly made conscious choices to purchase regulated goods online from unregulated sources, in some cases justifying their actions as a way to save money or obtain goods they could not otherwise procure.[11] During the pandemic, research has shown that the closure of physical retailers and many consumers' fears of being in close proximity to persons outside of their household has driven up the use of the Internet when it comes to purchasing regulated goods.[12] Simply telling people that this is a risky behavior that should be avoided is not enough, particularly when they have positive experiences that run counter to official messaging. Coronavirus related frauds have largely succeeded because people are willing to suspend their normal hesitations about engaging in certain behaviors. The force and influence of misinformation related to the legitimacy of certain activities, or questions about how trustworthy is legitimate messaging, are reinforced through consumers' increasing reliance upon alternative news sources for information.

One of the greatest challenges to the prevention of fraud is having the ability and resources to get reliable information to consumers in a timely fashion with a message that resonates and leads the consumer to take an appropriate course of action. The latter part of this statement is of utmost importance, particularly given the fact that it is incredibly easy to create

[10] https://a-capp.msu.edu/article/the-sociotechnical-evolution-of-product-counterfeiting-how-social-media-social-networks-and-social-commerce-are-e-socializing-product-counterfeiting/
[11] https://journals.sagepub.com/doi/abs/10.1177/0002764217734264?journalCode=absb
[12] https://buysaferx.pharmacy/research-us/

superficial appearances of legitimacy. I continue to believe that the success of any new or existing pandemic-related fraud scheme rests on criminals' ability to regularly, and in an uninterrupted fashion, interact with consumers in ways that prey upon a lack of information, consumer' distrust of official messaging, and fears about the virus. Our research on COVID fraud victimization found that low self control was a key predictor of being a victim of a virus-related fraud. The inability to determine the legitimacy of a source, distrust of official messaging and the propensity to take risks and seek short-term solutions all aid in the success of coronavirus frauds that rely upon alternative and deceptive messaging.

A Need to Protect the Most Vulnerable Populations

Crime is not randomly distributed, which means that the risks of victimization are not equally disbursed across society. For many crimes, victimization tends to concentrate within particular groups wherein vulnerability is greatest. This is especially the case with crimes like fraud that are financially drive and relatively stable in their operation over time. Because the coronavirus is a global pandemic it is easy to assume that its impacts, including the risk for fraud victimization, are also global in nature. This is not the case. The fraud victimization risks that have developed during the COVID-19 pandemic are not equally distributed. In some cases, victimization risk concentrates because of the ways in which money is distributed according to the dictates of financial assistance programs, such as the CARES Act. In other cases, victimization risk is concentrated within groups of people who engage in certain behaviors, such as the individuals looking for alternative medical treatments. In still other cases, victimization risk comes as a result of demographic characteristics that have become the focus of fraudsters.

Irrespective of how risk develops there is a need to acknowledge and address how vulnerability has led to a concentration of fraud risks.

When the CARES Act was enacted in the summer of 2020, stimulus check related frauds were acknowledged to be a clear and present danger to the individuals who would be receiving paper checks[13], as well as those who were unfamiliar with how to provide the information needed to receive direct deposits. We saw that individuals who had not recently filed a tax return (younger people, those on the lowest ends of the socio-economic spectrum, and immigrants) were targeted by scammers and thieves whose sole purpose was to steal stimulus funds. Additionally, older adults who had recently filed their taxes but were unsure of whether their information was on file were targeted by fraudsters seeking to steal sensitive personal information through Internet-based frauds. The unemployed were also targeted by frauds seeking to steal personal information and unemployment benefits, as phony websites purporting to offer assistance with signing up for benefits and federal assistance sprouted up almost overnight.

The speed with which these frauds developed is in large part due to the fact that fraudsters have been able to employ the same methods and techniques they have used in the past. Since the beginning of the pandemic consumers have been under constant pressure from frauds because the individuals who perpetrate these schemes already had their playbooks written. They simply needed to follow the script with a new group of victims. As the initial phases of vaccine distribution appeared, criminals again came seeking the individuals looking for priority access to the vaccine by setting up fraudulent and very legitimate looking websites designed to steal consumers' information.[14] Successful individuals and businesses have not even been spared from

[13] Singman, B. (2020, April 20). How to spot a counterfeit stimulus check: Secret Service, Treasury warn against coronavirus relief fraud. Fox News. Retrieved from https://www.foxnews.com/politics/spot-counterfeit-stimulus-coronavirus.

[14] Tressler, C. (2021, January 27). Scammers cash in on COVID-19 vaccination confusion [Blog post]. Retrieved from the Federal Trade Commission: https://www.consumer.ftc.gov/blog/2021/01/scammers-cash-covid-19-vaccination-confusion

the fraud risks that have developed during this pandemic, as PPP Loan scams have targeted small businesses funds and sensitive information.[15]

Protecting consumers who are at increased risk of victimization requires a dynamic approach to risk assessment, one that appreciates the fact that any group could become targeted for victimization. The Department of Justice[16] at one point suggested that the groups most likely to be targeted include those who have already been victimized by identity theft, those who have had their personal information exposed in a past data breach, and individuals who gave out their personal information in response to solicitations inquiring about help with filing unemployment insurance claims. While I wholly agreed with this statement at the time, the focus of current protection efforts must center on today's and tomorrow's vulnerable populations. Importantly, the messaging that needs to be disseminated must prompt self-protective behaviors and encourage consumers to seek assistance from legitimate authorities.

Finally, the work that my colleagues and I have conducted on COVID-19 frauds identified several important relationships that are worthy of note. First, two out of five people reported feeling targeted by frauds at some point in the first months of the pandemic; a statistic that is likely to have drastically increased by this point. Supporting the Department of Justice's suggestions, our findings indicated that people who had been victims of white-collar crimes in the past were more likely to be targeted by COVID frauds, as were younger people and those earning middle-class incomes. More than a quarter of people – one in four – admitted to having actually purchased a COVID-19 related product or service in the early months of the pandemic. These individuals tended to be living in a residential or nursing home, to have been a victim of a previous white-collar crime, and to have made prior purchases from telemarketers. We also

[15] https://www.sba.gov/about-sba/oversight-advocacy/office-inspector-general/protect-yourself-scams-fraud
[16] www.justice.gov/coronavirus

found that the people who purchased a COVID-related product were more likely to do so primarily because they were concerned that they would contract COVID.

Concluding Thoughts

I would like to thank Chairman Clyburn, Ranking Member Scalise and the entirety of the Select Subcommittee for inviting me here to testify on these issues. As you continue your incredibly important work, I would ask that you keep in mind the fact that successful fraud schemes tend to follow established solicitation patterns that place an emphasis on reassuring potential victims of the legitimacy and legality of the scheme.[17] The use of legitimate-appearing healthcare professionals and medically-focused websites is a prominent theme of current COVID scams. Additionally, the widespread nature of virus misinformation and disinformation means that many consumers are unlikely to heed government warnings about risky activities because they view official sources as lacking trust. When frauds involve the purchase of a product or the exchange of personal information guardianship factors can weaken and the risks for fraud victimization can increase.[18] While online, consumers are at an incredible information disadvantage relative to fraudsters[19] and during a healthcare crisis people tend to cope with the uncertainty by searching for things that make them safe and secure.[20] Legitimate information about the virus has been co-mingled with steady streams of misinformation and false information, making it difficult for some consumers to know what is real from fake.

[17] Holt, T. J., & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, *1*(1), 137-154.

[18] Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

[19] Kennedy, J. P., & Wilson, J. M. (2017). Clicking into harm's way: The decision to purchase regulated goods online. *American Behavioral Scientist*, *61*(11), 1358-1386.

[20] Gui, X., Kou, Y., Pine, K. H., & Chen, Y. (2017, May). Managing uncertainty: using social media for risk assessment during a public health crisis. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 4520-4533).

To address future fraud victimization risks, I would recommend that the government continue to strengthen consumer protections within the virtual world, particularly that which can exist across multiple platforms. Additionally, the use of "soft interventions"[21], such as warning systems that alert users to potentially misleading or risky messaging or products, may help to reduce consumers' risky online behaviors, as well as educate, empower and ultimately protect consumers. It may also be helpful to utilize public-private partnerships to curate and disseminate white-lists and black-lists that can be easily accessed by consumers as a guide to help them identify which individuals and sites are to be trusted and which should be avoided. The model developed for Internet pharmacy verification websites, which is operated by LegitScript (www.legitscript.com) and the National Association of Boards of Pharmacy (www.nabp.pharmacy), may be a good point of reference for such lists. Finally, it is necessary that consumers be given clear and concise messaging that comes from multiple sources of legitimacy, including those beyond official channels. Partnering with corporations, social media influencers, and other influential groups can help to strengthen the legitimacy and adoption of fraud prevention messaging.

Once again I thank you for this opportunity, and look forward to answering any questions you may have.

[21] Kariyawasam, K., & Wigley, S. (2017). Online shopping, misleading advertising and consumer protection. Information & Communications Technology Law, 26(2), 73-89.