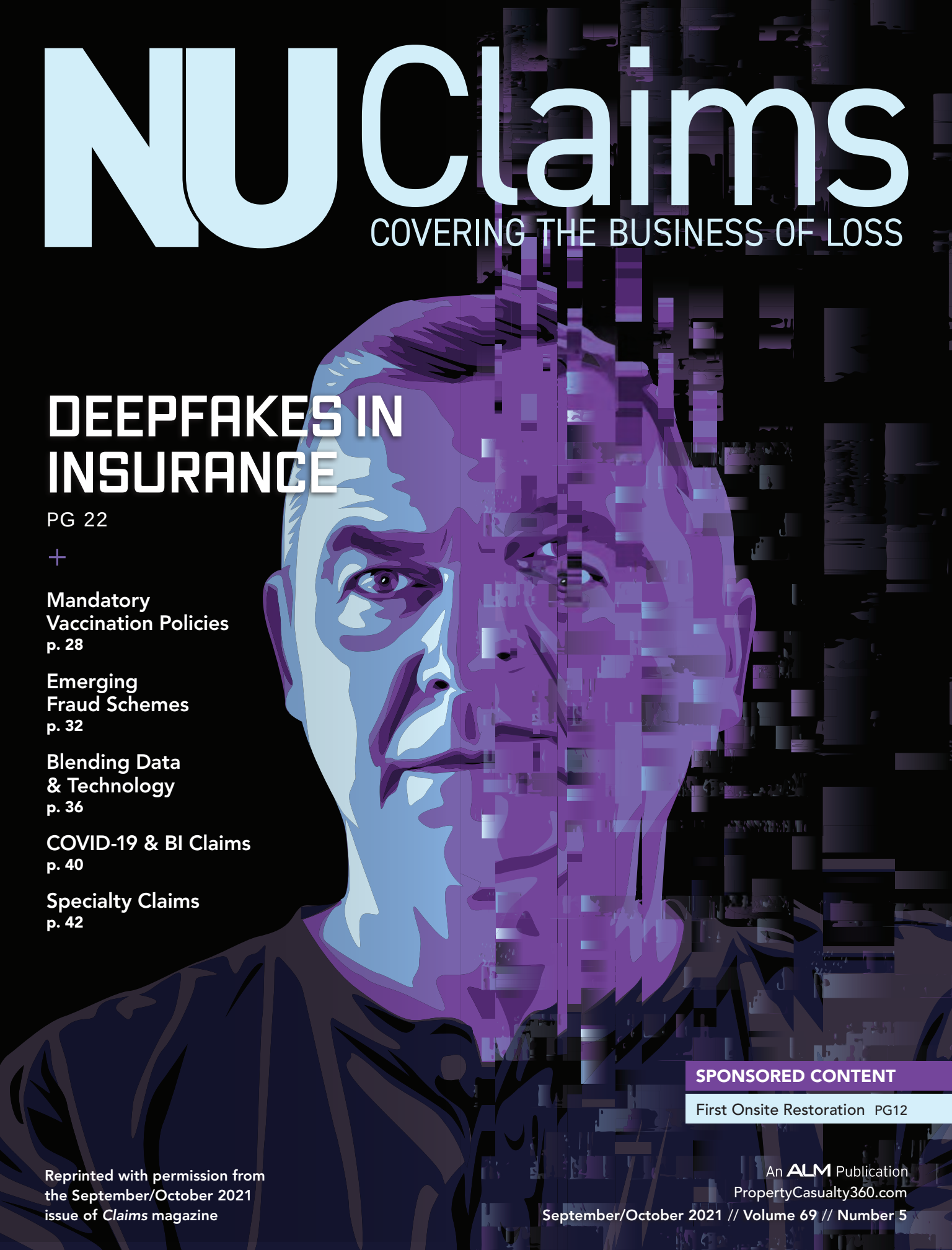
NU Claims
COVERING THE BUSINESS OF LOSS



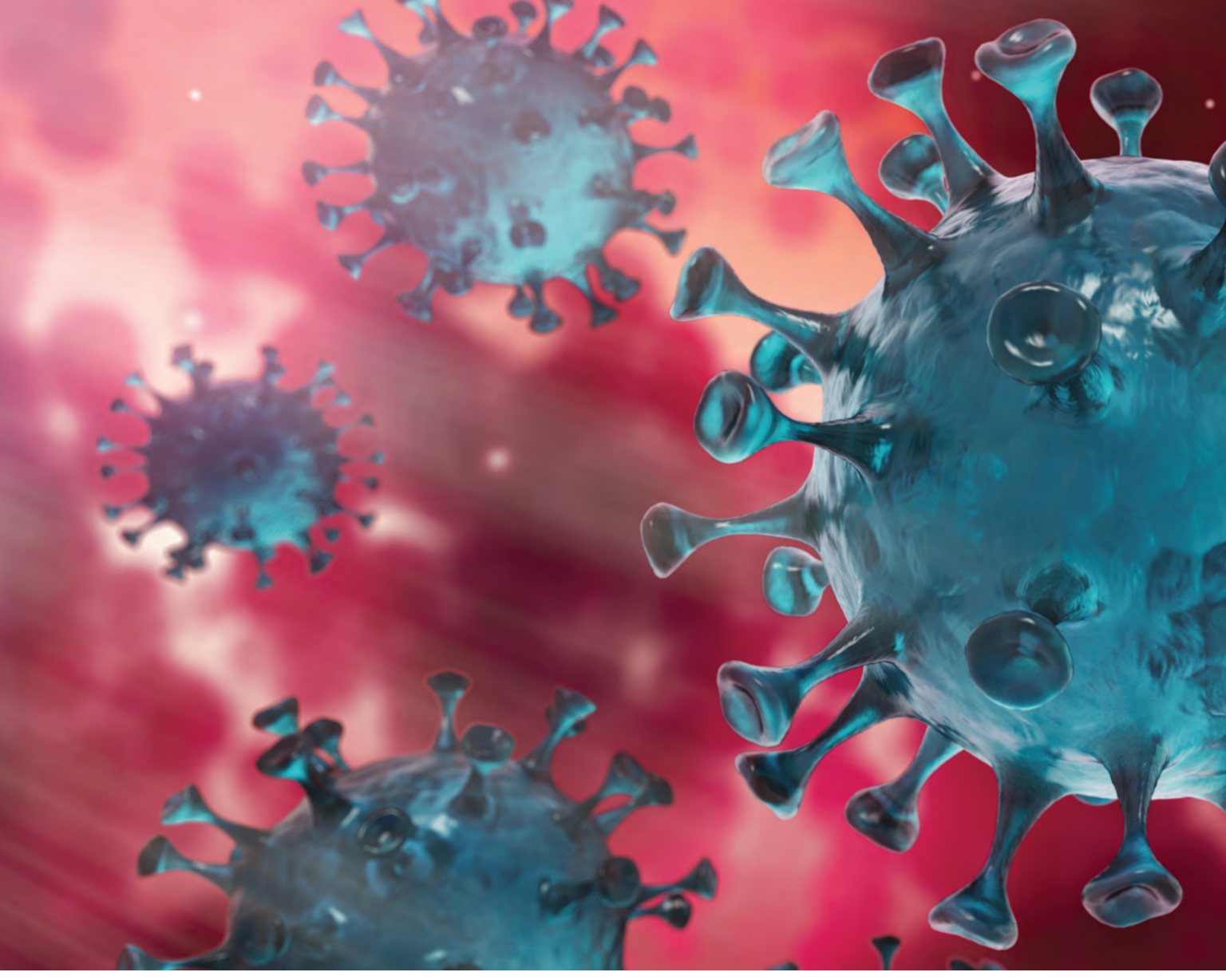
DEEPFAKES IN INSURANCE

PG 22

+

Reprinted with permission from the September/October 2021 issue of *Claims* magazine

An ALM Publication
PropertyCasualty360.com
September/October 2021 // Volume 69 // Number 5



ANOTHER CORONAVIRUS VARIANT: RADICAL FRAUD

By Richard Wickliffe, CPCU

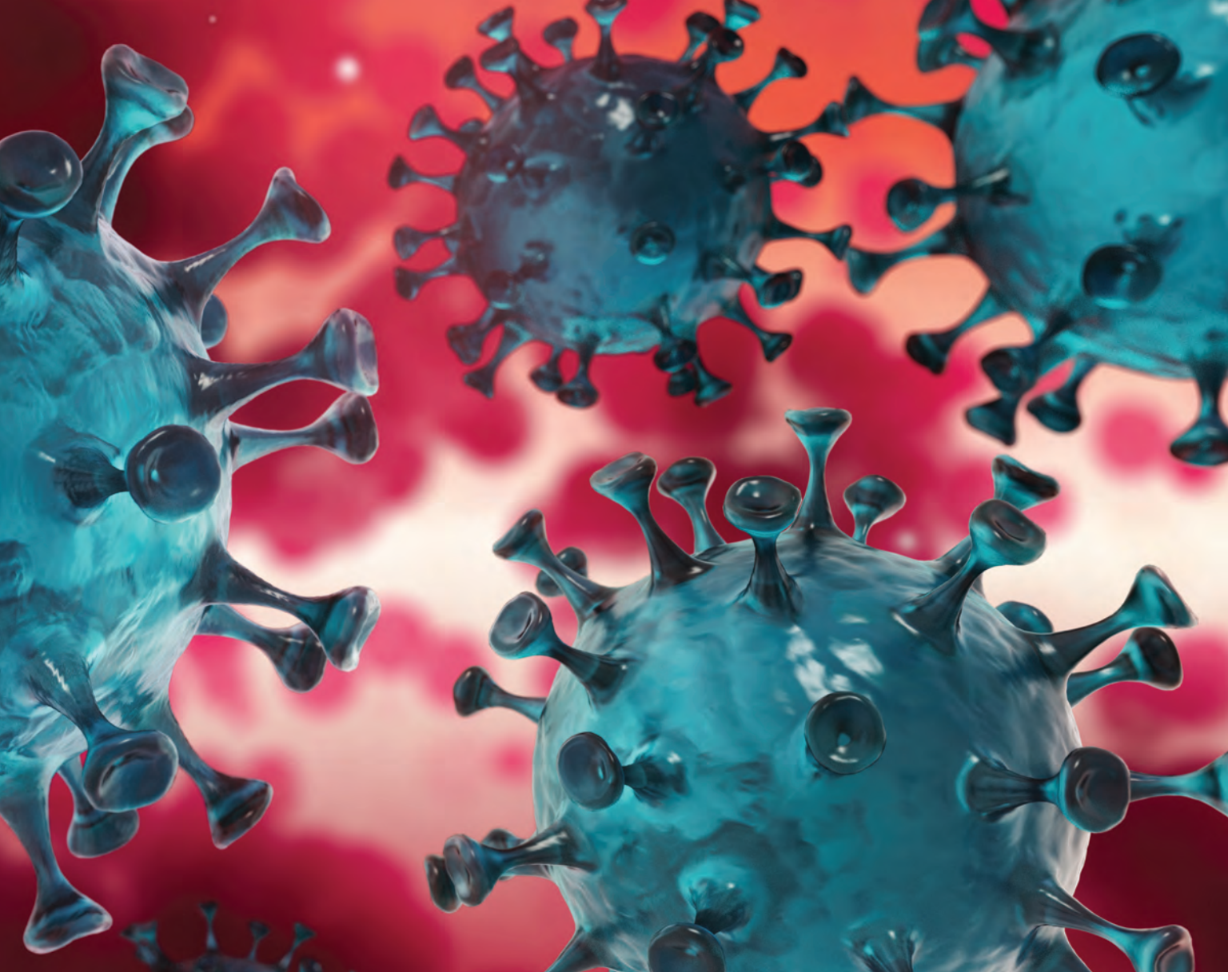
ACCORDING TO THE FBI, CON ART-ists are using the COVID-19 pandemic — including ensuing vaccines, variants and stimulus funds — for perpetrating multiple varieties of fraud.

One example is the marketing of fraudulent COVID-19 antibody tests for the sole purpose of amassing personal information, which is used for ID theft and insurance-related schemes.

Other tactics include the fraudulent advertising — through texts, social media and robocalls — of high-demand supplies such as facemasks, testing kits and cleansers. With variant strains and renewed mandates for masks, these trends will not be going away anytime soon. The Federal Communications Commission has issued warnings to numerous questionable firms and has created a dedicated website with information on COVID-19 phone scams.

STOCK MARKET FRAUD

The pandemic has also generated opportunities for fraud within the stock market. The U.S. Securities and Exchange Commission recently issued warnings to potential investors about fraudulent companies touting products that purportedly



prevent, detect or cure COVID-19. A July 6, 2021 warning for an "Earn Cash Quarantine Lending" consulting company boasts a 300% profit in 75 days.

The unscrupulous brokers suggest their clients "buy now" before prices skyrocket. With the manipulative "pump and dump" scheme, the fraudsters have already accumulated the firms' stock, sometimes for cents on the dollar. The hype then escalates the stock's value, so the perpetrators can dump the stock, burdening the investors with heavy losses.

CYBER FRAUD OPPORTUNITIES

According to a March 2021 report by Palo Alto Networks, a cybersecurity company, cybercriminals have registered tens of thousands of coronavirus-related web domains to use in spoof ads and phishing attacks. According to the report, the U.S. Department of Justice (DOJ) has shut down hundreds of these sites, which promise relief benefits, protective gear and vaccines and are often disguised as federal agencies or charitable organizations.

A self-proclaimed data expert called "Dustyfresh" has been updating a daily feed of bogus-corona-related domains, such as "CoronoVirusUpdate.com." If a victim were to visit one of the malicious sites, they might start receiving phishing emails in an attempt to gain personal data or plant malware to seek private files to access passwords and personal information for identity theft purposes. Fake sites have mimicked ads from Pfizer, Moderna and AstraZeneca, promising "free" rewards for providing bank or credit information to cover a small "handling fee."

FRAUD COMMITTED FROM JAIL?

In July 2021, a grand jury in Fresno, California indicted three incarcerated men for a scheme to submit over $1.4 million in fraudulent unemployment insurance claims in other inmates' names to the California Employment Development Department. The men were charged with conspiracy to commit mail fraud and aggravated identity theft. Their applications claimed the inmates had worked as clothing retailers, handymen and other jobs before coronavirus-related layoffs, and have been available to work (despite being in prison).

To avoid detection, the defendants created fake email accounts and used physical mailing addresses scattered throughout Southern California. Some paid friends and family up to $1,000 each to use their home mailing addresses.

According to a Federal Trade Commission (FTC) report, as of July 26, 2021, they'd logged over 561,000 consumer complaints related to COVID-19 and stimulus payments. Nearly 75% involved fraud or identity theft. These scams have cost consumers $505.25 million, with a median fraud loss of $373. The schemers' tactics closely mirror the constantly changing headlines, adapting their methods as new health and economic issues arise worldwide.

STIMULUS AND HEALTHCARE FRAUD

Some U.S. states have adopted vaccine lotteries to help people get their COVID-19 shots — with a renewed push with the coronavirus variants. Suspicious calls, texts and emails have been reported, offering cash in exchange for personal or financial information to expedite access to vaccines. The July 2021 FTC alert warned about a new wave of stimulus scams as the government plans to send advance child tax credit payments to millions of eligible families as part of the $1.9 trillion American Rescue Plan Act of 2021.

The Office of the Attorney General (AG) is working as fast as it can. From 2020 alone, the AG issued a report announcing the DOJ had negotiated more than $1.8 billion in healthcare fraud settlements from fiscal 2020. The DOJ opened 1,148 criminal healthcare fraud investigations and 1,079 civil healthcare fraud investigations. According to the report, COVID-19 had heavily expanded the fraud risks to federal health programs.

One example involved the billing for unneeded services, offering COVID-19 tests to Medicare beneficiaries in exchange for personal data including Medicare information. In one scheme, labs targeted retirement communities by offering COVID-19 tests, but then drew blood and billed the government for medically unnecessary services. Other schemes involved excessive lab testing, needless respiratory tests, allergy and genetic tests.

A telemarketing broker was charged for a scheme to bill Medicare for cancer genetic tests (CGX) and COVID-19 tests that were not eligible for compensation. The broker confessed how she and her accomplices had paid kickbacks to telemarketers who obtained CGX tests from Medicare beneficiaries who had doctors' orders authorizing the tests. They would send the completed CGX tests, along with the doctors' orders, to a lab which would then bill Medicare. In return, the broker received kickbacks from the laboratory. The fraudulent scheme totaled over $3 million.

According to a Federal Trade Commission (FTC) report, as of July 26, 2021, they'd logged **over 561,000 consumer complaints related to COVID-19 and stimulus payments**. Nearly 75% involved fraud or identity theft.

COVID-RELATED SCHEMES TO WATCH OUT FOR:

- Bogus remedies. Since the beginning of the pandemic, fraudsters have pitched phony remedies. Though vaccines have been distributed, the scam to purportedly help symptoms and immunity is unlikely to subside.
- Any request to pay out of pocket, or give personal information, to receive an injection or gain access to a vaccine "waitlist."
- The U.S. Food and Drug Administration has sent warnings to companies selling unapproved products that claim to prevent COVID-19, including teas, essential oils, cannabinol, colloidal silver and intravenous vitamin-C therapies. Sometimes marketed as "defenses" against the pandemic.
- Stimulus checks — beware of calls, texts or emails claiming to be from federal agencies that ask you to click a link, pay a fee, or "confirm" personal data such as your Social Security number to expedite a stimulus check.
- Viral schemes that promise COVID-19 relief financial "grants," requiring a link to be clicked, or the submission of personal information.

Bad actors will continue to find new ways to use real-life events for nefarious purposes. Having an awareness of how they operate can help reduce the incidence of fraud.

Richard Wickliffe, CPCU, ARM, CLU, (RLWickliffe@yahoo.com) has worked in the insurance industry leading teams of fraud investigators for over 20 years. He is the recipient of the FBI's Exceptional Service in the Public Interest Award and the author of crime fiction, where he has been awarded Best Popular Fiction by the Florida Book Awards.