protiviti®
Face the Future with Confidence

Preparing for a Dynamic Post-Pandemic Fraud Landscape

Inasmuch as COVID-19 has dramatically changed the lives of people, organizations, technologies, processes and workflow for just about every industry, it has been a tremendous boon to criminal enterprises. The disruptions from the unfolding global health emergency have created an unprecedented opportunity for fraudsters to carry out often-sophisticated, technology-enabled illicit schemes targeting vulnerable individuals, corporate networks and even government institutions.

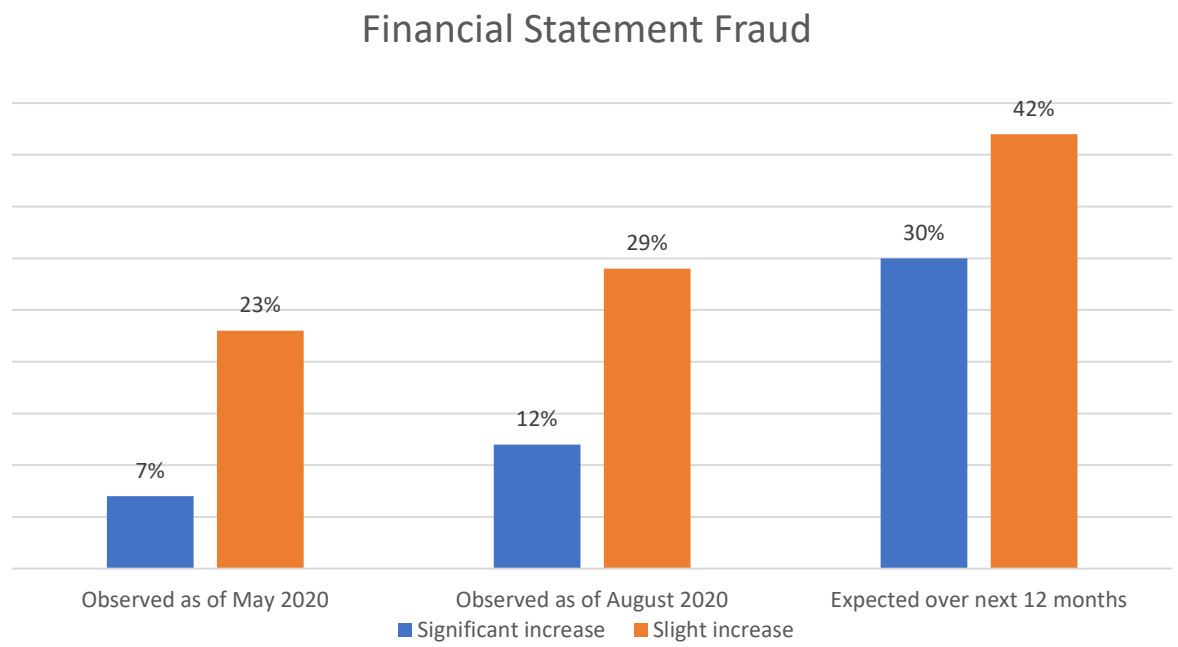
From the onset of the pandemic in 2020, law enforcement agencies and regulators began to send warning signals about the steady rise in fraud cases. Nearly a year and half later these incidents have continued unabated and, if the past is any indication of what is to come, they are likely to escalate in the coming months.

Billions of dollars in relief funds doled out to curb the pandemic have been the most significant driver of fraud so far, but there has also been an uptick in more traditional forms of fraud that typically emerge during an economic downturn. The combination of the health scare, financial hardship and greed created a perfect opportunity for crimes such as phishing scams, unemployment fraud, and schemes involving medical equipment supplies and fake charities.

Although the health crisis might be easing, the fraud landscape remains dynamic, prompting these questions: What can companies expect relating to fraud and regulatory oversight in the post-pandemic environment? What will the new normal look like?

As shown in the graph below, a poll conducted with members of the Association of Certified Fraud Examiners shows the number of fraud cases observed have been rising since May 2020 and almost three quarters of the polling participants expect the cases to keep growing.

Complaints to CFPB mentioning *coronavirus* or related keywords, by month.



Source: Association of Certified Fraud Examiners

Fraud Without Borders

Organizations should prepare for a post-pandemic fraud landscape that is rampant with transnational organized crime groups capable of attacking from anywhere around the world. In the past year and half, these organized groups have adapted to a world with restricted travel and closed borders by migrating to the cyberworld. These groups are heavily engaged in criminal activities such as loan sharking, counterfeiting of durable medical equipment and fake cure scams, malware attacks and exploitation of the elderly.

Indeed, the dark underworld of cybercrime has been thriving during the pandemic. According to research from Trustwave SpiderLabs, the volume of dark web users surged more than 40 percent in the early months of the pandemic, with an estimated $100 million in COVID-19-related goods and services — from fake vaccines to personally identifiable information (PII) stolen through COVID-themed phishing attacks — trading through these channels.

A recent survey from BAE Systems Applied Intelligence supports this escalation in pandemic-related cybercrimes. This survey found that 74% of financial institutions experienced a significant spike in threats linked to COVID-19. The upward trend is particularly worrisome because the institutions surveyed acknowledged they have reduced security, cyber-crime, fraud or risk department budgets by 26% in the past 12 months.

The Law in Hot Pursuit

Expect aggressive enforcement initiatives in pursuit of persons and companies that misappropriated federal dollars to continue after the pandemic. These initiatives, which may also target state sponsors of fraud, will emanate from all levels of government, including various international, federal and state and the various regulatory agencies.

In a sign that these actions are ramping up in the United States, U.S. Attorney General Merrick Garland announced on May 17, 2021, the formation of an interagency COVID-19 Fraud Enforcement Task Force. Compared to a similar task force created last year, the new body is different in terms of its formality and organizational structure; its goal is to bring together the resources of the Department of Justice (DOJ) and agencies throughout the federal government to fight fraud and protect the integrity of government funds. Specifically, the task force will investigate various forms of fraud, including individuals and entities that have:

- Capitalized on scarcity to peddle fake vaccines and sell millions of counterfeit N95 masks and other personal protective equipment to health care facilities desperate to protect frontline workers.
- Inflated their payrolls to obtain loans larger than they were eligible to receive.
- Used shell companies and received assistance that they unlawfully diverted.
- Set up operations to submit identical loan applications in the names of multiple companies.
- Fraudulently misrepresented the products or services they sold to the federal government.

Federal enforcement actions have already yielded arrests and prosecutions of perpetrators of COVID-19-related fraud activities. The following are just a sample of the actions reported recently.

- On May 27, 2021, The Wall Street Journal reported that in the past week alone, federal prosecutors have charged about a dozen people with pandemic-related fraud schemes whereby medical professionals submitted fake claims or bundled expensive and unnecessary tests with those coded as COVID-19-related.
- In April 2021, the Federal Trade Commission assessed its first monetary fine under the COVID Consumer Protection Law to a chiropractor and his company. According to the complaint, the defendants marketed vitamin D and zinc products under the brand name "Wellness Warrior," and claimed that they were as effective as, or more effective, than vaccines that are currently available.
- The DOJ charged 474 people in March 2021 with trying to steal more than $569 million in COVID-19-related fraud scams. The fraud section of the DOJ's Criminal Division charged an additional 120 defendants with Paycheck Protection Program fraud for inflating payroll expenses to obtain larger loans than those for which they would have qualified, reviving dormant corporations or purchasing shell companies with no actual operations to apply for multiple loans, and falsely reporting the size of their payroll. The

most common fraud involved misappropriated loan proceeds for personal uses such as the purchase of houses, cars, jewelry, and other luxury items.

- The DOJ reported that fraudulent funds totaling $580 million were seized as criminals targeted Economic Injury Disaster Loans by applying for advances and loans on behalf of ineligible, newly created, shell or non-existent businesses and diverting the funds for illegal purposes.
- The National Unemployment Insurance (UI) Fraud Task Force, established by the DOJ, is investigating and prosecuting the theft of more than $860 billion in federal funds appropriated from UI benefits through September 2021. According to the department, organized criminal groups are using stolen identities to file for UI benefits, with more than 140 defendants charged and arrested so far.

In April 2021 alone, the Federal Trade Commission (FTC) directed 30 marketers to stop making claims that their products and therapies can effectively prevent or treat COVID-19, bringing the total number of warning letters sent to nearly 400, according to the commission.

The ramping up of enforcement actions by the FTC, the DOJ and others is a clear indication that regulators and law enforcement agencies will continue to leverage all the tools at their disposal to make examples of noncomplying companies and to generate as much press coverage as possible in their pursuit of alleged fraudulent behavior. Companies that fail to comply and mitigate fraud risk severely damaging their brand and reputation.

What Companies Should Do Now

Today's dynamic environment calls for institutions to keep abreast of law enforcement, and regulatory and legislative changes, as well as reassess their compliance and fraud-prevention practices regularly to strengthen areas like third-party service arrangements where gaps in oversight can easily enable fraud.

Firms should also look to partner with industry groups that will keep them informed on fraud trends and counter-fraud measures. The insurance industry, as an example, does this effectively through its Coalition Against Insurance Fraud, a Washington, D.C.-based organization that is responsible for keeping its members informed on legislative and regulatory changes, as well as fraud activities, enabling them to partner with insurance commissioners in each state to develop effective counter measures.

Additionally, these broad strategies can help organizations strengthen their fraud prevention practices:

- **Conduct risk assessments to identify threat vectors**. Organizations that have not updated or completed a new risk assessment should do so as soon as possible. They should consider bringing in an independent party to give an unbiased assessment of fraud risks, assessing the likelihood the risk could occur and identifying how these risks would impact the organization.

- **Deploy advanced analytics to generate augmented insights that can be translated into intelligent threat detection and decision-making**. This process cannot be done without fully understanding data types and how to use them effectively to unlock the potential of any fraud surveillance and monitoring system. In most cases, firms can capture and use existing metadata for this process.
- **Incorporate machine learning and artificial intelligence tools to detect suspicious behaviors, including anomaly detection**. Text-mining tools can be deployed to uncover patterns in unstructured data and predictive models can evaluate common activities against known cases of misconduct.
- **Collaborate internally and externally with key stakeholders**. Sharing experience and intelligence on fraud trends across the company and industry on a global perspective will provide firms with a 360-degree view of threat vectors and anomalies.
- **Be vigilant**. Business leaders cannot be overly cautious in this environment. They should keep their eyes and ears open for warning signals and make sure that all employees across the enterprise — not just the guardians of information and IT systems — are up to speed on fraud-detection measures because they constitute the real front line against these crimes.

To learn more about how COVID-19 has become a breeding ground for fraud, read these additional insights from Protiviti:

- Hard Times Bring Out the Best in People – Well, Not Always
- COVID-19 - A Breeding Ground for Fraud
- Managing Financial Crime Risks in a Changing Economic Environment

Contacts

Jill Smiley
Director, Risk & Compliance
+1.704.972.9611
jill.smiley@protiviti.com

Dennis Toomey
Director, Risk & Compliance Analytics
+1.603.494.2736
dennis.toomey@protiviti.com