How 3rd Parties Can Best Limit Fraud Liability Amid COVID-19

By **Robyn Crowther and Ashwin Ram** (April 14, 2020)

Robyn Crowther

Ashwin Ram

As state and federal authorities crack down on opportunistic price-gouging and fraud born out of the COVID-19 crisis, innocent third parties who provide a platform or the means to facilitate this activity may get caught in the crossfire.

Third parties in this context potentially include the entire supply chain other than the actual seller in the price-gouging context or the actual conspirators intending to deceive or cheat consumers in the fraud context.

No business is exempt, and affected companies range from online vendors to advertisers and even voice over internet protocol providers, who share the misfortune of having their services misappropriated to facilitate price-gouging or fraud.

Given the broad threat to the status quo, companies should be aware of the latest developments underlying this enforcement activity, evaluate risks giving rise to potential civil and criminal exposure, and implement best practices for mitigating such risks.

Recent Developments and Trends

The COVID crisis has led to a surge in enforcement activity targeting fraud and pricing-gouging. On the state level, approximately two weeks ago, 34 state attorneys general sent letters to prominent online retailers calling on these companies to take a harder stance against price-gouging amid the COVID-19 pandemic. A number of these online retailers are already defending against such claims.

The federal government is also aggressively policing fraud, hoarding and price-gouging associated with the COVID-19 crisis. On April 3, the Federal Trade Commission and Federal Communications Commission took a first-of-its-kind step to warn three VoIP providers — providing the equivalent of digital phone services — that if they did not implement immediate changes to stop COVID-19 phone scams against consumers, the agencies would tell U.S.-based phone carriers to block certain calls routed from these VoIP providers.

Moreover, last month the U.S. Food and Drug Administration and FTC issued warning letters to several companies for selling fraudulent COVID-19 products, including unapproved drugs that could pose significant risks to patient health.

More broadly, on March 23, President Donald Trump issued an executive order that prohibits hoarding designated items for the purpose of selling such items in excess of prevailing market prices. On the heels of executive order, the U.S. Department of Justice formed the COVID Fraud Task Force.

U.S. attorney's offices across the country have started designating experienced federal prosecutors to be a part of the task force, which has already publicly launched a handful of investigations involving health care kickbacks, investment fraud, and fake COVID cures, testing kits and masks.

Potential Liability for Third-Party Companies

COVID-19 enforcement activity raises the specter that companies — ranging from online vendors, advertisers and even VoIP providers — facilitating the sale of exorbitantly priced products, or providing the means or mechanism for others to engage in fraudulent activity, may be exposed to potential civil and criminal liability.

Although a variety of legal theories could be asserted to bring about this potential liability, there is significant uncertainty associated with any such claims. For example, what is the requisite intent or mental state required for a company or individual to be liable? Strict liability exists in both civil and criminal cases but is generally only applicable to a limited category of cases such as public welfare offenses in criminal law and inherently dangerous or defective products in civil cases.

Given this uncertainty, companies in the supply chain should take proactive steps to avoid claims that they acted knowingly, recklessly or even negligently with respect to facilitating the sale of offending products or fraudulent schemes.

This is particularly important given the ubiquitous nature of price-gouging and fraud during the COVID-19 crisis and the availability of catch-all legal theories such as vicarious liability and inchoate offenses such as conspiracy and aiding/abetting. Indeed, exposure may even come from within companies, with shareholder derivative actions seeking proactive corporate policies and reforms.

With respect to criminal enforcement activity, state investigators will likely continue to focus on actual wrongdoers, but the standards on which wrongdoing is based may be a shifting goal post in times of crisis.

Fortunately, innocent third parties in the supply chain for price-gouging and businesses whose facilities are otherwise used to commit fraud are not without potential defenses. For example, online retailers, advertisers and other third parties are not the actual sellers of the offending products or activity.

Section 230 of the Communications Decency Act, a federal law, protects websites from liability stemming from the traditional editorial functions of a publisher — such as deciding whether to publish, remove or edit posts or other content generated by third parties.

But the degree of control or involvement an online retailer or third party exercises in a sales transaction may impact the availability of the defense. Additionally, a company's actual or constructive knowledge that it was facilitating fraud or price-gouging activity may also limit the viability of such a defense.

Best Practices for Third-Party Companies

Based on the barrage of recent enforcement activity, companies involved in the supply chain of high-demand products essential to fighting the COVID-19 pandemic, as well as companies that may be able to readily identify fraudulent activity, must do more than simply condemn the use of the at-issue facility to commit fraud or price-gouging.

It is critical for companies to take proactive steps to limit and prevent such sales and activity. The March 25 letter from 34 state attorneys general to various companies with strong online presences helpfully provides a roadmap of best practices to consider:

- Set policies and enforce restrictions on fraudulent activity and price-gouging;

- Trigger price-gouging and fraud protections prior to an emergency declaration, such as when online systems detect conditions such as pending weather events, precipitous stock market declines or future potential health risks; and

- Implement a complaint portal for consumers and insiders to report potential fraud and price-gouging.

These practical solutions will help reduce the risk that a company in the supply chain or part of a communication platform may unwittingly facilitate fraud or price-gouging. Adopting these best practices will also help a company demonstrate good-faith compliance to regulators and simultaneously mitigate potential civil and criminal exposure.

Robyn Crowther and Ashwin Ram are partners at Steptoe & Johnson LLP.