By Sandy B. Garfinkel, Esq.
Member, Eckert Seamans Cherin & Mellott, LLC

I. Re-Opening and Room Rates: Beware of Price Gouging Laws

So-called "price gouging" is when a business providing essential consumer goods or services takes advantage of abnormal market conditions caused by events such as natural disasters, armed conflicts or other crises, by raising prices to excessive levels. To date, 35 U.S. states have enacted anti-price gouging legislation. Typically, these statutes make it an illegal act for a business to raise prices or rates for essential goods or services during an emergency. In most cases the laws impose specific price limitations for essential items or services where a state of emergency has been declared, and those limitations commence immediately upon the publication of a state of emergency by a governing official.

Lodging is considered an essential consumer service under anti-price gouging laws. Some state statutes specifically identify hotels and motels to be providers of essential services, and these laws contain specific language addressing how hotels and motels must restrict their rates while the limitations are in effect.

The COVID-19 crisis resulted in the largest number of declarations of emergency the country has ever seen, at every governmental level. Many of them are still in effect. Others may be reinstituted should the number of viral cases increase. As re-opening proceeds, Hotels may be tempted to make large rate adjustments to offset revenue losses due to the crisis. Hotels must take care to understand whether they are: (1) in a state with an anti-price gouging law, and (2) whether an active state of emergency still exists.

State attorneys general are the regulatory enforcers of price gouging laws. During investigations, hotels are required to disclose comparative room rate data to investigators. The issue is complicated by the fact that many hotels set rates on a semi-automated basis using systems that track demand and "comp set" rates published by competing hotels, and in those circumstances room rates may fluctuate beyond the imposed statutory limits without hotel personnel controlling the fluctuations. Moreover, investigators are not always aware of nuances in the hotel industry that should fairly be taken into account when deciding what comparative rate data to use as evidence. Responding to investigations can be time-consuming and expensive.

Here are steps that hotel companies can take to protect themselves:

- <u>Have a policy and a practiced procedure</u>. One person should act as an alert system if a state of emergency is declared, and should notify any properties in that state.

- Learn the laws. Price gouging laws differ from jurisdiction to jurisdiction in terms of what factors trigger them, how prices should be constrained and for how long.
- Document everything. Documentation is key because you may have to make some judgement calls. Document that you have a procedure in place that complies with the law, you made an effort to follow that procedure, and all of the decisions you made about rates were informed.
- Stay on top of passive rate adjustment tools. Many properties use passive rate-setting revenue management systems. During a state of emergency these must be monitored to make sure the automatic system is not establishing rates that will be in violation of price gouging statutes.

II. Data Privacy and Security Challenges During Re-Opening

The COVID-19 crisis and stay-at-home orders drastically changed corporate cybersecurity landscapes within an extremely compressed period of time. Almost every industry, including hospitality, rushed to introduce or increase the use of remote technology tools for work-related communication, including:

Video Conferencing	Group Chat
File Sharing	VPN
Virtual Desktops	Web-Based Applications and Tools

Cyber criminals wasted little time exploiting these rapidly-introduced changes, which produced cyber vulnerabilities from hasty or non-existent policies, training, risk assessments, and systems testing. Remote access controls, including safe login credentials and multi-factor authentication, have not been universally adopted by businesses, and fraudsters have successfully lied or hacked their way into home computers, stealing credentials and accessing sensitive work systems. Clever fraudsters have also capitalized on chaos and fears surrounding the virus outbreak, creating false narratives to entice individuals into clicking on links or attachments promising information on disease transmission, treatments and testing. PPP program frauds, stimulus program fraud and widespread unemployment compensation scams emerged. As a result, news sources have reported an increase in cybercrime ranging from social engineering/credential stealing to ransomware to business e-mail compromise.

Returning employees to work will cause more confusion, at least in the short term. By and large, returning to work will be done gradually or in phases. That will mean reactivating on-site networks and systems while maintaining remote access protocols, resulting in more chaos and more opportunities for

cyber mischief. Stolen credentials stockpiled by cyber thieves and malware hidden in systems during the course of the lockdown period can be expected to be activated and utilized by cyber thieves over the coming months.

On the privacy side, coinciding with efforts to reopen the economy is the impending July 1, 2020 enforcement kickoff for the **California Consumer Privacy Act (CCPA)**. The California Attorney General will begin investigating and pursuing businesses covered by the CCPA for noncompliance. The CCPA is a sweeping privacy law loosely modeled after Europe's GDPR, with some major differences. The CCPA gives Californians rights over their personal data collected by businesses, including the right to demand deletion and that the business not sell the individual's personal information. To the extent hospitality companies are doing business in California and meet certain other criteria, they must quickly prepare the appropriate privacy statements and employee disclosures, and ready processes to respond to consumer information requests in a timely and fully-compliant fashion.

Many hotels across the country have announced plans to perform temperature scans on individuals entering the premises. Operators and owners need to be aware that thermal data constitutes protected biometric information under the CCPA. If the hotel is covered by CCPA and the individual is a California resident, the hotel cannot collect temperature readings without first making required disclosures. Even outside the context of CCPA, hotels must be careful about collecting and sharing healthcare information about guests, so as not to run afoul of other laws restricting those activities.