From July 2013 to June 2014, there were 87 terror attacks on hotels worldwide. Additionally, in 2015, ISIS claimed responsibility for the attack at the Hotel Riu Imperial Marhaba in Tunisia. Companies that invite access to the public, particularly those with brands associated with US business and culture, have become targets. This article describes the legal standards applicable to the assessment of the liability of lodging providers in the event of a terror attack. In addition, it addresses risk management both from the perspective of the contract terms governing the operation of hotel and resort assets, as well as governmental accreditation, designation and certifications that are available to mitigate or eliminate liability. Finally, the article recommends certain strategies to be considered in the event that a lawsuit is filed, as well as highlighting the key future threats to the financial viability of hotel assets.

**TERROR ATTACKS INVOLVING US HOTEL BRANDS: AN EXAMPLE**

On the evening of September 20, 2008, a truck loaded with explosives rammed through the gate barrier of the Marriott Islamabad Hotel in Pakistan. The attempt to breach the barrier was unsuccessful. However, the truck caught fire and exploded, killing 56 people and injuring approximately 270 more. The Marriott Islamabad was a franchise hotel owned and operated by Hashwani Hotels, a Pakistani corporation. Among the dead was Albert DiFederico, a US citizen and civilian contractor working in Pakistan, who was a guest at the hotel. His widow and three sons later sued Marriott in Maryland where the company is headquartered, alleging that inadequate security had led to DiFederico’s death and that Marriott was responsible. The DiFederico’s did not sue the Pakistani franchisee or anyone else.

Marriott initially succeeded in having the Court dismiss the case on the basis that it was more appropriately brought in Pakistan. However, an appellate court reversed. Marriott again sought to dismiss the case arguing that as a franchisor it had no duty to the guests of a franchisee, and, therefore, no legally valid claim had been made against it. The trial judge refused to dismiss this time. In so doing, the court expressed some concern that the allegations against Marriott needed to be stated...
Protecting Hotel Industry Businesses from Liability for Terror Attacks

with more specificity and eventually proven, but allowed the case to go forward with the attendant risk of a lengthy and expensive multi-year litigation process. In fact, the litigation continued until September, 2015, when the federal court in Maryland ultimately dismissed the plaintiffs’ claims, finding that Marriott did not exert sufficient control over the operations of the hotel to make it responsible for Mr. DiFederico’s death. However, the case is not over yet, as the plaintiffs have appealed.

The Islamabad Marriott bombing highlights the risks faced not only by owners of hotel properties but also by the companies who extend licenses to owners for the use of their hotel brand. Indeed, owners, managers, franchisees, and everyone’s subcontractors are all potential hotel industry defendants.

TRADITIONAL LIABILITY RULES APPLIED IN AN AGE OF TERROR: THE CHALLENGES

A hotel or other innkeeper (“inn” remains the legal term for a hotel, motel, bed and breakfast, or other lodging place) has a duty to use due care to protect its guests against hazards that are foreseeable, including criminal acts. In practical terms that means a hotel has a duty to take precautions that are reasonable in relationship to the likelihood that without them guests will be victims of criminal acts. This traditional rule is based on the concept that the hotel has better access to information about the danger than its guests, enabling it to take preventive measures. This basis has been the rationale for a rule in some, but not all states in the United States, that a hotel or other “innkeeper” has an elevated standard of care toward its guests. For example, in Virginia, an innkeeper has an elevated duty of “utmost case and diligence” to protect a guest from criminal acts of third parties. The District of Columbia, on the other hand, uses a “sliding scale” analysis to determine if a duty exists to a guest for third party criminal acts. The two ends of the scale are: (1) the criminal act’s foreseeability, and (2) the degree to which the hotel owes a “greater duty of protection” by nature its relationship to the victim. In the absence of a protective relationship, the plaintiff must make a “heightened showing” of the criminal act’s foreseeability to establish a duty. Conversely, a relationship “entailing a greater duty of protection” lightens the plaintiff’s burden to show foreseeability.

Based on the nature of the foreseeability test and its different versions, it is clear that there is no bright line test controlling liability to guests. In applying the District of Columbia “sliding scale” rule, one court recently found that the hotel manager did owe the victim of an assault a “greater duty of protection by virtue of the innkeeper—guest relationship.” The Court noted that the guest need not make a “heightened showing” of foreseeability but still had to make “some showing” that the assault was foreseeable. The Court ultimately entered judgment on behalf of the manager because the guest had failed to provide adequate evidence of the assault’s foreseeability. Specifically, the Court found that evidence of the surrounding area’s crime rate and unrelated incidents at the hotel did not suffice to show that the manager should have foreseen the attack.

Interestingly, the Court further reasoned that even if the assault were foreseeable, the plaintiff’s evidence did not establish the “requisite standard of care.” To establish the standard of the care the guest had used an expert witness. The Court found “vague, passing references” by the expert to “best practices,” “articles by security experts,” and “certain minimum standards” to be insufficient. Further, the Court noted that the expert conceded that there “are no uniform national standards governing hotel security measures.”

These legal rules have evolved in the context of domestic crimes and not international terrorism. Their application in the context of terror attacks has been limited and the results that the courts will reach in applying the rules in an age of terror still remains largely an open question. There is some precedent stemming from the attack on the World Trade Center in September, 2001. In one lawsuit arising from the September 11 attacks, the Court rejected an attempt to dismiss the case by the owners of the World Trade Center who claimed they had no duty to the victims. The Court noted that the “difficult question is whether the injuries arose from a reasonably foreseeable risk.” In applying the foreseeability test and refusing to dismiss the case, the Court noted that the plaintiffs alleged that owners could have reasonably foreseen crashes of airplanes into the Towers because of a near miss in 1981 by an airplane; studies conducted during construction addressing whether the Towers would be able to withstand an aircraft crash (and concluded they could); numerous fires and evacuations that occurred at the Towers since their opening; and “the common sense assumption” that the World Trade Center likely continued to be a prime target of terrorists. The court stated “a defendant has to have been aware of a specific hazard” but “[i]t is
Protecting Hotel Industry Businesses from Liability for Terror Attacks

As terror attacks continue and grow in number, hotel owners, operators, and other “innkeepers” are likely to face more robust arguments that the incidents were foreseeable. Further, in the absence of uniform national standards governing hotel security measures, the analysis of each case will be fact intensive and depend on factors such as prior relevant incidents, the location of the premises, any specific threats made, compliance with governmental regulations, compliance with the lodging provider’s own policies and procedures and the effectiveness of any protections implemented.

The legal standards described above are US based. However, to complicate matters, it is possible that in a case involving a terror attack in a foreign country that is brought in the US Courts, the plaintiffs will request that the US Courts apply and interpret foreign law instead of US law. In the Marriott Islamabad litigation, for example, the federal District Court in Maryland entered an Order in June, 2015 requesting that the parties address the following question regarding a franchisor’s potential duty to hotel guests:

Under Pakistani Law, under what circumstances can an individual maintain a cause of action against a franchisor injured on the premises of franchisee that owns and operates the premises, whether based on negligence, agency, estoppel, or any other legal theory?6

In seeking to dismiss the case, Marriott had argued that Pakistan was a more convenient venue to hear the case. In support of that argument, Marriott contended that it would be a “daunting, burdensome” task for a court in Maryland to apply Pakistan’s laws. The federal appellate court rejected this argument stating that “this is precisely the kind of work American judges perform on a daily basis.” Based on at least this decision, there is no guarantee that the claims of terror victims will result in those claims being heard in foreign courts in the country where the attack happened. If the claims are heard in US Courts, the foreign law of the country where the attack occurred may apply to all or some of the issues in the case.

Against this backdrop of fluid legal standards and potentially applicable laws of other countries, how risk is allocated contractually is a crucial consideration as discussed below.

ALLOCATING RISK THROUGH THE TERMS OF HOTEL FRANCHISE AND MANAGEMENT AGREEMENTS: SELECT KEY CONTRACT TERMS

The escalating attacks against hotels and resorts make the review and analysis of existing hotel related contracts and future prototypes even more critical in terms of how the responsibility for harm is allocated. This analysis discusses contract terms that allocate risks among franchisees, franchisors, owners, and operators for the claims of guests and business invitees.

In an attempt to obtain a dismissal of the Islamabad case, Marriott continued to argue that the franchisee, Hashwani, was not Marriott’s agent pursuant to the express terms of the franchise agreement. Further, Marriott asserted that it could not be responsible legally for the franchisee’s acts because it did not exert day-to-day control over Hashwani and had no relationship with the company Hashwani hired to train and oversee security officials.

On the other hand, the plaintiffs argued that Marriott closely developed and monitored all security measures at the Marriott Islamabad. They pointed out that Marriott hired a former Green Beret with the US Army Special Forces to form a crisis management team. That team was charged with the duty to assess risk and implement measures to handle the threat of terrorist attacks for all properties in the Marriott chain, including the Marriott Islamabad. In addition, the plaintiffs asserted that Marriott controlled security measures because it developed training plans for the employees of its franchises. Because of these measures, plaintiffs urged the Court to rule that Marriott had a duty under Pakistani law to the Hotel’s guests and was liable if it performed that duty negligently.

In September, 2015, the Court dismissed the plaintiffs’ claims, finding that Marriott had not exerted control over Hashwani’s day-to-day operations or otherwise exerted sufficient control to create a duty to hotel guests. Further, the Court found no reliance by the decedent on the franchisor’s mark. It noted that there was no evidence that Mr. DiFederico decided to stay at the hotel in question because of the Marriott brand or that he relied on the adequacy of Marriott’s security procedure. The Court ruled that this lack of evidence was “fatal” to plaintiffs’ claims that Marriott was liable on theories of agency by estoppel or apparent agency.
DiFederico demonstrates that the ultimate responsibility may rest with the franchisee hotel owner and not the brand for terror attacks, unless the victim demonstrates that it relied on the brand. Hotel investors and owners should be aware of this risk calculus when they enter into franchise agreements and plan accordingly.

The risk of catastrophic events caused by terror attacks also requires a careful analysis of force majeure clauses in hotel contracts. The goal of a force majeure clause is to allocate risk and to regulate when the contracting parties performance is excused. Today, there is arguably an increased risk that terrorism will be considered foreseeable, and therefore is excused. To today, there is arguably an increased risk that terrorism will be considered foreseeable, and therefore failure or delay in performance due to terrorism may not be excused unless terrorism is specifically listed in the force majeure clause of franchise and management agreements.

All too frequently, force majeure clauses are considered mere boilerplate in a contract. However, recent events illustrate the necessity of assessing these types of provisions carefully. Following a terror attack, operators may find that meeting a contractual performance test is an unsurmountable hurdle. From an Owner's perspective, the Operator's performance may be based in whole or in part on events other than the terror attack and the Owner may opt for termination based on performance failure. It is important that the force majeure clause provide clarity on what events trigger a force majeure and what the consequences of that trigger will be.

Contractual provisions relating to the repair and restoration of hotels after catastrophic events frequently have been treated as boilerplate. Increasingly, over the last few years, draconian repair and restoration provisions have crept into hotel contracts, particularly in the international context and in emerging markets. These provisions basically commit owners to a complete rebuilding of an asset, regardless of the extent of destruction and the availability of insurance proceeds. Accordingly, an astute evaluation of repair and restoration terms in a contract is an essential component of risk management and allocation in an age of terror. Even in more standard, less draconian provisions than those just described, the owner and operator must consider issues such as what the damage threshold for repair is and whether the owner has the right to terminate the management agreement without a payment of compensation to the existing operator and start anew. Further, if the management agreement is terminated, these are certain key issues to address, namely, whether the owner and operator will share any insurance proceeds and if so, in what proportion; will the operator have a right of reinstatement if the hotel is rebuilt after a terror attack; and is the operator entitled to receive any form of compensation if it is not reinstated.

Finally, and importantly, no discussion of potential liability in the hotel industry in an age of terror would be complete without a consideration of indemnity clauses. The indemnity provisions in hotel contracts have not received much attention in the ongoing discussion regarding liability for terror acts against hotel industry assets. However, those provisions directly impact the shifting of the risks of a terror attack between owners and operators. For example, indemnity provisions in management agreements increasingly provide that owners indemnify operators for liabilities associated with the asset, with the exception of liabilities arising out of gross negligence or the intentional misconduct of employees. In other words, the owner indemnifies the operator for its negligence. In an age of terror, these indemnity provisions take on added significance as operators face claims that, but for their negligence, the injuries and damages resulting from terrorism would not have occurred. Owners should anticipate that where contracts contain indemnities for the operators’ negligence, operators will seek to have owners absorb the liability for any alleged operator negligence. At that juncture, the factual dispute between owners and operators is likely to shift to whether an operator’s conduct constituted gross negligence or willful behavior, which conduct would fall outside the ambit of traditional indemnity clauses found in hotel contracts.

Many current hotel agreements were executed prior to September 11. Their indemnity provisions should be evaluated through the prism of worldwide terrorism and what it may mean to an owner to be responsible for the negligent behavior of an operator. At a minimum, owners should consider inserting exculpatory clauses into contracts to protect themselves. A traditional exculpation clause in a hotel management agreement resembles the following:

Notwithstanding any other provision of this Agreement to the contrary, the liability of Owner arising out of or in connection with this Agreement and the transactions and obligations contemplated hereby shall at all times be limited to the interest of Owner in the Hotel, and in any litigation or any other dispute, neither Manager nor any other party shall seek or have recourse to any other asset of Owner or to Owner’s partners, members, associates, agents, executives or Affiliates. Without limiting the foregoing, neither Owner nor any party associated with
Owner shall have any liability in excess of Owner's interest in the Hotel for any act by Owner, including liability for the gross negligence, willful misconduct (either prior to or during term of or after the expiration or earlier termination of this Agreement) or breach of this Agreement by Owner.

SAFETY ACT DESIGNATION AND CERTIFICATION AND OTHER STANDARDS AND ACCREDITATIONS: TOOLS TO MITIGATE OR ELIMINATE LIABILITY

While contract terms that allocate the risk of liability from terror attacks are essential, it is also important that lodging providers assess the options available to them to mitigate or eliminate that risk in the first instance. The assessment below focuses on certain of those options.

Safety Act Designation and Certification

Providers of lodging services should consider using the Safety Act.9 While not a magical shield against liability for terror attacks, the Safety Act does provide some real protection against the potentially crippling financial liability that could come in the aftermath of an attack.

The Safety Act was passed by Congress in 2002, as another response to the September 11 attacks. It originally was seen as a way to encourage development and use of anti-terrorism technology. The Safety Act did so by providing liability protection for sellers and users of that technology, when approved by the government. The Department of Homeland Security (DHS) conducts assessments and keeps a list. Importantly, “technology” is defined very broadly to include not just mechanical equipment such as bomb scanners, but security services and procedures as well. For example, the “New York Yankees Security Program,” and the “NFL Best Practices for Stadium Security” have been deemed “technology” and have received accreditation under the Safety Act. The previously mentioned new security procedures for major league professional baseball games are part of its recent certification. Somewhat surprisingly, a recent review shows few other “public” entities have sought certification. There are no hotel companies on the list.

Under the Safety Act, sellers and users of “technologies” (again, including programs) that have been approved by the DHS are granted liability limitations. These liability protections will apply if the Secretary of DHS determines that there has been “an act of terrorism,” defined as an act that: (1) is unlawful; (2) causes harm to an entity in the United States (even if the act itself occurs outside the United States); and (3) is designed to cause mass destruction, injury, or other loss to US citizens or institutions.

There are two levels of protection in the Safety Act depending on the type of approval DHS has granted: (1) “designation,” and the higher level of (2) “certification.” For those technologies and procedures that have received “designation” under the Safety Act:

- Liability is capped at an amount of insurance coverage that DHS specifies must be carried (though DHS cannot require insurance in excess of industry standards);
- Plaintiffs’ claims may be brought only in federal court (which often is a significant advantage to defendants);
- No joint and several liability is allowed for non-economic damages (meaning that if several defendants are liable and there is a way to allocate responsibility, no one defendant, (e.g., the one with the most assets) will be asked to pay the entire amount of nonspecific and potentially very high “pain and suffering” damages);
- No punitive damages or pre-judgment interests are allowed; and
- Plaintiffs’ recovery must be reduced by those amounts received from collateral sources (e.g., insurance payouts), which is not the law everywhere.

For technologies that have received “certification” under the Safety Act, the seller or user of the “technology” receives all the benefits of designation above, plus:

- The government contractor defense can be invoked to potentially preclude liability entirely. This defense provides that where a private entity manufactures a product or delivers a service pursuant to and in compliance with detailed government specifications, it is not liable for any tort resulting from the product or service; and
- The technology is placed on DHS’s public “approved products list,” potentially affording the seller or user marketing advantages.

Some additional “technologies” that recently have received these designations include: Dow Chemical’s Rail...
Transportation Security Plan, Five Star Airport Alliance Inc.'s plan for baggage screening, the Port Authority of New York and New Jersey’s La Guardia Airport Security Program, and the International Council of Shopping Centers, Inc. Terrorism Awareness Training Program.

Obtaining Safety Act approval is neither easy nor quick. In deciding whether to grant approval the DHS Office of Safety Act Implementation considers many factors, including the extent of the terrorism risk to the public, the likelihood that the technology will not be deployed absent Safety Act approval, and the demonstrated effectiveness of the technology.

Approval is likely to be situation specific. For example, a hotel chain owner might find it difficult to persuade DHS that a more limited security plan likely to be effective in the United States, will be equally effective in a war torn or politically unstable area. To pass muster the security plan for the more dangerous area probably will have to contain more stringent elements. Security Act approval is not a for-gone conclusion and may require considerable investment. Yet, given the human and financial risks, the cost of failing to consider Security Act approval may conceivably be steep. Indeed, failure to apply for or achieve Safety Act approval could even potentially be cited in and of itself as a failure of a standard of care, particularly if a competitor or comparable provider of services has received approval.

Standards and Accreditations

There are many private commercial entities that will review companies and facilities and issue security “accreditations.” In addition, the DHS has a “Commercial Facilities Section Specific Plan,” as part of its “Natural Infrastructure Protection Plan.” DHS will make security recommendations to owners and operators of commercial facilities. The current DHS program includes such features as site assistance visits, Web based security assessment applications, bomb making awareness training, and other measures. DHS does stress that the ultimate responsibility for security lies with facility owners and operators, but its mission is to help.

Consulting with appropriate authorities and following recommendations and codes of conduct would be useful evidence of due care in the event that claims are made. Indeed, as discussed below, in the context of data security breaches at certain Wyndham branded hotels, a federal court ruling regarding the Federal Trade Commission’s (FTC) claims against Wyndham demonstrate the importance of consulting the published guidance of regulators.

RISK MANAGEMENT WHEN A LAWSUIT HAS BEEN FILED: SELECT RECOMMENDATIONS

There are procedural guideposts that a hospitality industry provider should consider if sued in the wake of a terrorist incident. First, consider whether there is a more preferable US legal forum available. If hotel operators or owners are sued in a particular court, it is likely that the plaintiff chose it because it is perceived to be a pro-plaintiff venue. If an innkeeper is sued in a state court and there is a basis to remove the case to federal court, careful consideration should be given to an evaluation of the respective benefits of proceeding in state versus federal court.

Next, a jurisdictional question that often arises in international terrorism cases is the doctrine of forum non conveniens. This legal rule basically provides that a court may dismiss a case if it more logically belongs in a foreign court. If a terrorist act has occurred at a hotel in another country and the case is filed in the United States, a lodging provider should evaluate seeking a dismissal that requires adjudication in the foreign country. The court will decide such a motion based on a variety of factors, including the availability of the evidence and witnesses, the state of the law and administration of justice in the forum, and the general convenience of the parties.

A number of courts have dismissed terrorist cases filed in the United States on forum non conveniens grounds, including a claim against Hyatt Corporation relating to a suicide bomber attack in Jordan10 and claims relating to terrorist attacks on the Taba Hilton Resort in Egypt.11 However, in the Marriott Islamabad case, the Court declined to rule that the case should be heard in Pakistan, in part because it had become too dangerous in Pakistan to require a US terror victim’s family to litigate there. Lodging providers should anticipate that terror victims will make the same argument about the danger of the foreign venue that succeeded in the Marriott Islamabad case. This may signal a new era of increased foreign terror related litigation being litigated in the US courts, paving the way for victims to avoid the perceived difficulties posed by foreign venues. However, a lodging company should not automatically seek to litigate in a foreign venue. The choice of venue is a critical part of an effective liability mitigation strategy and requires careful consideration of a variety of issues, not the least of which is an assessment of bias in the particular foreign venue against a large US corporation or other US entities.
THE FUTURE: CYBER ATTACKS AND STOLEN CUSTOMER DATA

The next frontier regarding owner/operator liability to guests concerns cyber warfare waged against hotel and resort businesses. Indeed, in 2014 the Sands Hotel and Casino in Las Vegas became one of the first, if not the first, US business attacked by a foreign government seeking to destroy its corporate infrastructure. The perpetrator—eventually identified by the Director of National Intelligence as the Iranian Government—wanted to retaliate against the chief executive officer and majority owner of the Las Vegas Sands Corp., Sheldon Adelson. Adelson is one of Israel’s most ardent supporters and he made comments that angered Iran. Hackers penetrated the Sands’ systems through the Sands Bethlehem, a relatively minor player in the Sands’ corporate family located in Bethlehem, Pennsylvania. It is estimated that recovering data and building new systems as a result of the attack will cost $40 million or more. It also has been reported that customer data including social security numbers, drivers’ license numbers, and passport numbers were stolen.

The situation at the Sands demonstrates the evolving nature of the terror threat, the additional types of liability to which lodging providers may be exposed and the need for a strategy that encompasses available government safeguards and carefully evaluates contract terms in the context of new, unprecedented threats. The actions of the FTC with respect to customer data security underscore the immediacy of that need. In June, 2012, the FTC sued Wyndham Worldwide Corporation and three of its related entities after the hotelier suffered three data breaches that allegedly comprised the payment card information of more than 600,000 customers. The FTC alleged, among other allegations, that Wyndham’s failure to use encryption, firewalls, and non-obvious passwords constituted an “unfair” practice under Section 5 of the FTC Act. In August, 2015, a US federal appellate court agreed with the FTC in a decision that the FTC has stated is a “must read for business executives and attorneys.”

The Wyndham decision, although it did not deal with a terror attack, is a warning about the hotel industry’s need for cybersecurity preparedness in an age of terror, including consulting the published guidance of the regulators. In that regard, the Court in Wyndham noted that the FTC had issued a guidebook, Protecting Personal Information: A Guide for Business, that counseled against many of the alleged practices of Wyndham, which the Court reasoned provided Wyndham with fair notice of practices to avoid.

As the Sands attack and the Wyndham case illustrate, the hotel industry by its very nature is at the epicenter of not just physical attacks by third parties but the growing threat of cyberattacks.

NOTES
8. Safety Act, including a full list of designations and certifications, see www.safetyact.gov.