New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 261—NO. 41

MONDAY, MARCH 4, 2019

Hardening **Cyber Protection** Programs

Will 2019 be the year of the SAFETY Act for data security programs?

BY CRAIG A. NEWMAN, PETER C. HARVEY, ALEJANDRO H. CRUZ AND JOSHUA R. STEIN

ROBERT KNESCHKE VIA SHUTTERSTOCK

An obscure federal statute, passed in the wake of the September 11th, 2001 terrorist attacks, grabbed big headlines last year when MGM Resorts International used the law to sue victims of the 2017 Las Vegas Harvest Festival shooting. Casino giant MGM, which owns Mandalay Bay Resort & Casino, the hotel where a shooter took up residence and killed 58 people in the deadliest shooting in U.S. history, sought a judicial declaration that the SAFETY Act—the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002—barred any claims against it.

MGM's litigation offensive might seem like an odd juxtaposition of legal strategy—suing the victims. Yet, despite public outrage over MGM's novel legal move, it represents the first time the SAFETY Act has been litigated, moving the cases and the enigmatic statute into uncharted legal territory, and will remain so for the foreseeable future. Shortly after MGM filed the lawsuits, it decided to switch gears and move from litigation to mediation. So, it is now behind closed doors working to hammer out a settlement rather

CRAIG A. NEWMAN *is a litigation partner and chair of the data security practice at Patterson Belknap Webb & Tyler.* PETER C. HARVEY *is a former Attorney General of New Jersey and a partner in the firm's litigation department, in which* ALEJANDRO H. CRUZ *is a partner and* JOSHUA R. STEIN *is an associate.*

than litigating issues of first impression which would serve as the only judicial precedent under the SAFETY Act.

While the issues raised by MGM's move might never be addressed if the cases are settled, it nonetheless underscores the fact that the SAFETY Act is likely to become a crucial—even essential—tool for qualified American companies' risk management and cybersecurity programs. And as the only instance in which the Act has been litigated, the MGM cases also provide a useful backdrop for taking a closer look these issues.

SAFETY Act Basics

The SAFETY Act, in general, provides legal protections to companies that develop cutting-edge anti-terrorism technologies, including cybersecurity programs, and are able to satisfy the demanding standards of the U.S. Department of Homeland Security (DHS), the agency that administers the SAFETY Act program. The Act has been on the books for years and more than 900 applications have been publicly approved since 2004.

Approval under the SAFETY Act comes with a variety of potentially powerful protections, including liability caps, market differentiation, and exclusive federal jurisdiction for certain claims. As companies become increasingly sensitive to the need for robust cybersecurity policies and procedures—both to protect digital assets and mitigate the liability that comes along with the near-inevitability of a data breach—the incentives offered to companies under the Act make it a potentially important component of their cybersecurity strategies.

To be sure, SAFETY Act protection is not for every organization. The qualification process is rigorous and not every organization will fit within the law's parameters, nor will they be able to meet its high standards.

The SAFETY Act requires companies to make detailed submissions regarding their technology and, following a rigorous certification process administered by DHS, they might become eligible to receive one of three possible levels of approval, each with varying benefits and timelines for protection.

If a company obtains approval at any level from DHS, the SAFETY Act provides a range of litigation management benefits that can substantially mitigate their cyber liability if the approved technology is deployed to protect against an act of terrorism. *First*, the Act provides for a single exclusive federal cause of action when the qualified technology is involved in an act of terrorism; this ensures that the company deploying or selling the technology will not be subject to duplicative and costly claims in different state courts. *Second*, the Act provides a liability cap based on the company's insurance coverage. If a company receives DHS approval, it is required to maintain liability insurance at a level set by DHS, but this cap adds a rare measure of certainty to litigation in which the Act's protections apply. *Third*, the Act bars the award of punitive damages, prejudgment interest, and joint and several liability for non-economic damages such as pain and suffering for claims.

Although the vast majority of SAFETY Act approvals so far have involved anti-terrorism products and services used for physical security, DHS has recognized that the universe of anti-terrorism technologies extends to an organization's cybersecurity program. DHS has broadly defined the scope of what can constitute a qualified anti-terrorism tech-

nology to include "any qualifying product, equipment, service (including support service), device, or technology (including information technology)."

For example, Southern Company, the Atlanta-based energy firm, recently obtained DHS certification for its "Cybersecurity Risk Management Program," an "enterprise-wide cyber risk mitigation program" that encompasses governance, network security, data protection, incident response, training, and policies, among other aspects. As cybercrime and data-based terrorism become an increasingly prevalent aspect of digital life, robust programs to harden a company's defenses against such threats have become a must-have aspect of corporate governance to manage an institution's potential liability, as well as that of its executive leadership team and board of directors.

Looking Ahead: Cybersecurity And the SAFETY Act

No doubt, the cybersecurity risks for companies that depend on sensitive information to drive their operations have soared. Hacking, phishing, and ransomware have become ever more sophisticated and commonplace.

And the price tag attached to cybersecurity incidents is astronomical. It is estimated that the cost of cybercrime globally will quadruple over the next four years from $500 billion to over $2 trillion. One recent study suggests that the average total cost of a U.S. data breach was nearly $8 million, and that a "mega breach," involving one million records or more, would have a cost of $40 million. Companies that obtain SAFETY Act approval for their cybersecurity programs take an important step in managing these and other economic and litigation risks.

There are, moreover, important non-statutory benefits to obtaining DHS approval under the SAFETY Act. Not only is it a "stamp of approval" from the U.S. government that an organization has achieved industry-leading cybersecurity protections, it establishes that the company and its leadership team took substantial steps to mitigate cybersecurity risks, which could be strong evidence, in and of itself, in litigation, whether against the company, its board of directors, or even with regulators.

Under the right circumstances, the SAFETY Act has the potential to become a new gold standard for companies that qualify for its protection and want to establish themselves as leaders in cybersecurity, both with respect to internal risk mitigation and with a view toward ensuring robust protection of customer or client data. In the face of cyberterrorism's growing threat, MGM's recent litigation predicament should serve as a wake-up call for institutions and corporate leaders aiming to be at the forefront of cyber-risk and liability management.