DICKSTEINSHAPIRO LLP

Global Security Practice

SAFETY ACT Capabilities

Dickstein Shapiro is one of the top law firms on the SAFETY Act. Since the enactment of the SAFETY Act, our attorneys have helped prepare a significant percentage of the applications that have been filed with the Department of Homeland Security.

With our industry-leading attorneys and significant experience in the field, Dickstein Shapiro's Global Security Practice is poised to help clients gain the valuable protections offered through a cutting edge approach to the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 (known as the SAFETY Act). This piece of legislation provides tort liability protections for products and services that can be used to detect, defend against, or respond to cyber attacks.

The SAFETY Act was implemented to respond to concerns by companies that they may be exposed to nearly limitless legal liability in the event of a cyber attack. Under the SAFETY Act, the owner or seller of cyber security products and/or services may apply for significant liability protections from the Department of Homeland Security (DHS). If a product or service receives SAFETY Act certification, then it is presumptively entitled to immunity from claims arising from a cyber attack. Under SAFETY Act designation, the tort liability is limited to the amount of insurance required to be maintained, as determined by the DHS. Under both circumstances, cases may be brought only in federal court.

Why Should I Worry about Liability from Cyber Attacks?

The proliferation of cyber attacks on all sectors of the U.S. economy has been staggering. At least 50,000 to 60,000 new pieces of malware are discovered on a daily basis, and companies in every economic sector have been attacked and suffered some form of loss. Companies have suffered the loss of personally identifiable information, had operations disruptions, lost valuable intellectual property, and have even been the victims of politically motivated cyber attacks. Unfortunately, the pace and intensity of these attacks only seem to be growing. Also growing is the litigation resulting from cyber attacks. Companies face litigation from affected individuals, and even from government agencies. New standards of care are being established and new disclosure obligations are potentially arising, especially in light of recent staff guidance from the Securities and Exchange Commission. It is easy to anticipate that, similar to claims relating to acts of terrorism, courts could hold that a cyber attack is a "reasonably foreseeable" event and that companies must take reasonable measures to mitigate the possibility of attacks. The problem is that there is no single definition of "reasonable" or "appropriate" cyber security measures. This leaves great uncertainty and creates a significant possibility of massive liability following cyber attacks.

How Can I Take Advantage of the SAFETY Act?

Any company or property owner that makes, sells, or otherwise deploys a cyber security product or service can and should seek SAFETY Act protections. The SAFETY Act represents one of the most efficient ways to proactively minimize or eliminate a company's liability exposure before a cyber attack even occurs. Companies can apply for SAFETY Act protections and can market them knowing that their liability exposure is limited under the U.S. Code. Buyers of cyber security tools and services can also take advantage of the protections because under the SAFETY Act they are not exposed to liability for claims arising out of or related to the use of the SAFETY Act approved products or services. So long as the products or services have some use against cyber attacks, they are eligible for SAFETY Act protections.

What is Eligible for SAFETY ACT Protections?

A wide variety of products and services are eligible for protections under the SAFETY Act. Examples of products and services that could receive SAFETY Act protections include anti-virus programs, firewalls, risk assessments, mobile security systems, mobile applications, information-sharing policies and procedures, and network monitoring services. Given the prevalent need for cyber security tools and their widespread use by terrorists and criminals, nearly all cyber security products are eligible for SAFETY Act protections.

Why Utilize Dickstein Shapiro to Obtain SAFETY Act Protections?

Dickstein Shapiro assists in the preparation, filing, and managing of SAFETY Act applications and does so effectively because of its unique level of experience working with clients on SAFETY Act-related issues. Dickstein Shapiro has helped prepare well over 100 of the applications filed with the DHS, making it one of the top law firms on SAFETY Act matters. Firm attorneys regularly write and speak on the SAFETY Act and have even testified before the House Committee on Homeland Security about the implementation of the SAFETY Act.

Representative Client Experience

Dickstein Shapiro professionals have assisted with a wide variety of SAFETY Act applications. Examples include obtaining SAFETY Act protections for:

- A professional sports league;
- Several software companies;
- The manufacturer of widely used airport screening devices; and
- A cutting-edge surveillance systems company.

Brian E. Finch is a partner and head of the firm's Global Security Practice. He was named by *Washingtonian* magazine in 2011 as one of the top 40 federal lobbyists under the age of 40. Mr. Finch also is a professional lecturer of law at the George Washington University Law School, where he co-teaches a class on homeland security law and policy. He is regularly quoted in publications such as *CQ Homeland Security* and *Washington Technology*, and has been profiled by *Government Security News* Magazine.

For further information, please contact:

Brian E. Finch
(202) 420-4823
finchb@dicksteinshapiro.com