

Letter to the Securities and Exchange Commission from 36 Organizations with an Interest in Trade Secret Protection

August 8, 2016

Mr. Brent J. Fields
Secretary
Securities and Exchange Commission
100 F Street N.E.
Washington, D.C. 20549-1090

RE: File No. S7-06-16; Release Nos. 33-10064; 34-77599 (Business and Financial Disclosure Required by Regulation S-K)

Dear Mr. Fields:

We are pleased to submit these comments in response to the Securities and Exchange Commission's ("SEC") Concept Release on Business and Financial Disclosure Required by Regulation S-K ("Concept Release")¹ on behalf of the 36 undersigned companies and organizations (hereinafter "signatory organizations"). Many of these organizations also participated in the Protect Trade Secrets Coalition ("PTSC"), a cross-industry group of companies and associations created in 2014 to advance legislation to close a gap in the federal Economic Espionage Act of 1996 by authorizing a federal civil cause of action for trade secrets theft and misappropriation.

In light of our shared view regarding the importance of trade secrets, these comments focus only on the potential impact of disclosure requirements relating to technology and intellectual property ("IP") rights, as discussed in Section IV(A)(3) of the Concept Release, on trade secret owners. In particular, these comments solely address the following question posed in Question 42 of the Concept Release as it would apply to trade secrets: "Should we expand the rule [the requirement under Item 101(c)(1)(iv) to disclose a registrant's patents, trademarks, licenses, franchises and concessions] to include other types of intellectual property...?" After careful consideration of this question, the undersigned organizations respectfully submit that the disclosure requirements under Item 101(c)(1)(iv) of Regulation S-K should not be expanded to trade secrets. We believe that such an expansion would provide no real benefit for investors while creating new risks and burdens for trade secret owners and would undermine recent achievements of this Administration to enhance trade secret protection in the United States and around the globe.

¹ [Business and Financial Disclosure Required by Regulation S-K](#), File No. S7-06-16; Release Nos. 33-10064; 34-77599 (Apr. 13, 2016).

Our arguments, as developed in more detail in the body of this letter, are as follows.

Collectively, we believe that the risks associated with adding trade secrets to the categories of IP subject to the disclosure requirements of Item 101(c)(1)(iv) would far outweigh benefits, if any, to investors. The risks to trade secret owners from such a disclosure requirement include the following:

- *Loss of trade secret protection by “over disclosure”.* In trying to comply with such a requirement and avoid SEC enforcement, a trade secret owner would risk disclosing information that could jeopardize the very secrecy that protects these valuable commercial assets. A trade secret has value precisely because it is secret.
- *Significant commercial harm.* Disclosure even of the mere existence of a trade secret could make such secrets a target for attempts at misappropriation, whether by a competitor directly, or through state-sponsored espionage. As a result, the proposed disclosure requirement could significantly discourage continued and new investments in innovation.
- *Undue compliance costs.* The requirement to disclose information about a registrant’s trade secrets would impose a significant burden on trade secret owners by requiring them to catalog all their trade secrets. This is particularly burdensome because doing so is not required to protect that IP right in the first place.

Moreover, by requiring trade secret owners to disclose an indeterminate amount of information about their trade secrets, the SEC not only might create significant competitive and enforcement risks for trade secret owners, but would also set a negative precedent globally at a time when the U.S. seeks to be a leader in the fight against global trade secret theft.

I. Background

The Importance of Trade Secret Protection

Trade secrets are owned by companies across all industries. They include information such as customer lists, proprietary technologies, formulas and codes, manufacturing processes, recipes and other innovations that often provide a primary competitive advantage to the trade secret owner. They also include sensitive product and marketing plans, research and development, and other business information that depends upon confidentiality to provide a critical business advantage. The development of trade secrets can represent months, years, or even decades of investment in research and development and know-how collected at a company. Whether such information qualifies as a trade secret depends on whether a trade secret owner has taken “reasonable measures to keep such information secret” and “the information derives

independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.”²

For many companies, trade secrets represent highly valuable business information. Trade secrets thus play a critical role in advancing U.S. competitiveness and driving economic growth.

A trade secret has value precisely because it is secret. Once a trade secret is unlawfully disclosed or obtained by a competitor without an obligation of secrecy its value is eroded, if not entirely lost. Such disclosure can allow a competitor to benefit from the originator’s often substantial investments in proprietary technologies or know-how, thereby undermining a trade secret owner’s incentives to invest further in new innovations. Moreover, technological advances and 21st century business models have made it easier than ever to facilitate trade secret theft. Losses stemming from trade secret theft are significant. The U.S. Department of Defense has stated that as a result of cyber espionage, every year, U.S. businesses, universities and government lose “an amount of intellectual property larger than that contained in the Library of Congress.”³ Meanwhile, a 2014 study suggested that trade secret misappropriation results in economic losses equivalent to 1% to 3% of U.S. GDP.⁴

Enhancing Trade Secret Protection: a U.S. Priority

Recognizing both the substantial value of trade secrets to the U.S. economy as well as their growing vulnerability, the United States has been at the forefront of promoting enhanced protection for trade secrets. In 2011, the U.S. Administration issued a White Paper on Intellectual Property Enforcement Legislative Recommendations that included several proposals for enhancing trade secret protections.⁵ Two years later, the White House released *The Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (hereinafter “2013 U.S. Administration Strategy”).⁶ This strategy recognized that while U.S. firms lead the world in

² 18 U.S.C. §1839(3).

³ Dep’t of Defense, *Strategy for Operating in Cyberspace*, at 4 (July 2011), available at <http://www.defense.gov/news/d20110714cyber.pdf>.

⁴ The Center for Responsible Enterprise & Trade and PricewaterhouseCoopers, *Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats*, at 3 (February 2014), available at <http://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf>.

⁵ *Administration’s White Paper on Intellectual Property Enforcement Legislative Recommendations*, (March 2011), available at https://www.whitehouse.gov/sites/default/files/ip_white_paper.pdf.

⁶ *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*, (February 2013), available at https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

research and development investments, foreign competitors had dramatically ramped up their efforts to steal the innovations that resulted from these immense investments by U.S. firms. The strategy found that this theft was putting American firms at a competitive disadvantage in the increasingly global marketplace, costing billions of dollars annually and thousands of domestic jobs. The strategy recognized that U.S. leadership was critical to protecting trade secrets both at home and abroad.

The United States took a significant step toward protecting trade secrets earlier this year with the enactment of the Defend Trade Secrets Act (“DTSA”), which provides a federal civil cause of action for trade secret misappropriation.⁷ The DTSA adds a civil analog to the Economic Espionage Act of 1996, which authorizes federal criminal prosecutions for trade secret theft. Although the criminal provisions of the Economic Espionage Act remain an essential foundation for the protection of trade secrets, in passing the DTSA, Congress recognized that, with limited resources, the responsible federal agencies could not respond to each and every instance of trade secret theft, and many such instances did not warrant a federal criminal response. Prior to enactment of the DTSA, private enforcement of rights in trade secrets was left to state laws, primarily the Uniform Trade Secrets Act.⁸ At the federal level, however, trade secrets were the only form of intellectual property for which there was no federal civil cause of action for misappropriation. Reliance on state law to protect trade secrets was cumbersome and inefficient in most cases in which the theft was interstate or, as was increasingly the case, international.

The DTSA received overwhelming bipartisan support among federal policymakers, passing the Senate 87-0 and the House, 410-2, with the strong support of the President, who signed the bill into law in May as Public Law 114-153.

The United States has also made advances to enhance trade secrets globally. The 2013 U.S. Administration Strategy highlighted the importance of trade negotiations and other trade tools to combat the use of trade secret theft by foreign governments or competitors to gain an unfair commercial advantage. Since that time, the Office of the U.S. Trade Representative (“USTR”) has included a trade secret section in its annual “Special 301 Report.” USTR’s 2016 report, for example, highlighted concerns with government regulations in certain countries that might require companies to disclose valuable source code that was protected as a trade secret.⁹ In addition, the U.S. was a leader in securing enhanced trade secret obligations in the recently-concluded Trans-Pacific Partnership Agreement (“TPP”), setting an important standard in the

⁷ The Defend Trade Secrets Act of 2016, S. 1890, sponsored by Senators Orrin Hatch (R-UT) and Chris Coons (D-DE) and 65 bipartisan cosponsors. Companion legislation, H.R. 3326, sponsored by Representatives Doug Collins (R-GA), Jerrold Nadler (D-NY), George Holding (R-NC), Hakeem Jeffries (D-NY) and 164 bipartisan cosponsors.

⁸ 48 U.S. states have trade secret statutes. 47 of those states have enacted the UTSA.

⁹ USTR, 2016 Special 301 Report, at 20 (Apr. 2016), available at <https://ustr.gov/sites/default/files/USTR-2016-Special-301-Report.pdf>.

Asia-Pacific region. Similarly, the United States is also seeking to elevate global trade secret protections through the ongoing Trans-Atlantic Trade and Investment Partnership (“T-TIP”) negotiations with the European Union.¹⁰

II. The Potential Impact of the SEC’s Proposed Increased Disclosure Requirements

It is against this backdrop that the signatory organizations urge the SEC not to adopt any disclosure requirements that would unnecessarily harm trade secret owners and run counter to the trade secret priorities of this Administration and Congress. In particular, and in response to the questions posed in the Concept Release, the signatory organizations do not believe that Item 101(c)(1)(iv) of Regulation S-K should be expanded to require disclosure regarding trade secrets.

Item 101(c)(1)(iv) currently requires registrants to disclose information about their “patents, trademarks, licenses, franchises and concessions.”¹¹ Collectively, we believe that the risks associated with adding disclosure of trade secrets would far outweigh benefits, if any, to investors.

The risks to trade secret owners from such a disclosure requirement include the following:

- *Loss of trade secret protection by “over disclosure”:* As noted above, a trade secret is protected to the extent its owner has taken reasonable measures to keep such information secret and the information derives independent economic value from being secret. It is unclear how much information would be required by the SEC to satisfy a disclosure requirement relating to trade secrets. In trying to comply with such a requirement and avoid SEC enforcement, a trade secret owner could risk disclosing information that would jeopardize the very secrecy that protects these valuable commercial assets. At the same time, given how ubiquitous trade secrets are, the amount of information that could be required to be disclosed would likely be overwhelming. Companies would be placed in an untenable position of trying to determine which information is material, while investors could be overwhelmed with irrelevant information. Imposing this requirement on U.S. listed companies could also put them at a distinct disadvantage to non-public companies, and to public foreign issuers (to the extent that their U.S. disclosure is not governed by Regulation S-K).
- *Significant commercial harm:* Trade secret misappropriation is a serious threat to U.S. companies. Business competitors around the world recognize the high value of U.S.

¹⁰ The European Union has also recently recognized the importance of trade secrets and the need to bolster legal protections for them by adopting the Directive of the European Parliament and of the Council on the Protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure. EU Directive 2016/943 (June 8, 2016).

¹¹ Item 101(c)(1)(iv) of Regulation S-K.

trade secrets. Unlike patents or trademarks, trade secrets do not require registration to ensure their protection. Thus, disclosure even of the mere existence of a trade secret could make such secrets a target for attempts at misappropriation whether by a competitor directly, or through state-sponsored espionage. The proposed disclosure requirement could, albeit inadvertently, significantly discourage continued and new investments in innovation.

- *Undue compliance costs:* In contrast to patents and trademarks, trade secret protection is not contingent upon registration. Thus, it is not the practice of most companies to catalogue all their trade secrets, which could be a considerably large undertaking depending on the size and nature of the company. It would seem unnecessary and inappropriate for the SEC to impose such a significant requirement on IP right holders, one that is not required to protect that IP right in the first place.

In addition, in light of the high-level priority this Administration and Congress have placed on protecting trade secrets, increased disclosure requirements would run counter to these U.S. policy goals. From support for the DTSA, to TPP, to increased attention to trade secret theft in the USTR Special 301 Report, this Administration and Congress have recognized the significant value of trade secrets to economic growth. The United States has sought to strengthen trade secret enforcement overseas and push back on any misuse of information submitted by trade secret owners to foreign governments in order to comply with safety and other product-related requirements. By requiring trade secret owners to disclose an indeterminate amount of information about their trade secrets, the SEC not only might create significant competitive and enforcement risks for trade secret owners, but would also set a negative precedent globally at a time when the U.S. seeks to be a leader in the fight against global trade secret theft.

* * * * *

Thank you for the opportunity to comment on the SEC's Concept Release. The signatory organizations urge the Commission to avoid the adoption of any disclosure requirements that would undermine trade secret protections and harm U.S. global competitiveness. We welcome any questions you might have about our submission.

Sincerely,

3M

Adobe

AdvaMed--the Advanced Medical Technology Association

Advanced-Manufacturing Coalition for Technology and Innovation (ACTI)

Autodesk, Inc.

Biotechnology Innovation Organization (BIO)

The Boeing Company

Boston Scientific

BSA | The Software Alliance

Caterpillar Inc.
Corning Incorporated
The Dow Chemical Company
Eli Lilly and Company
General Electric
IBM Corporation
Illinois Tool Works Inc. (ITW)
Information Technology Industry Council (ITI)
Johnson & Johnson
Leggett & Platt, Incorporated
Medical Device Manufacturers Association (MDMA)
Medtronic
Michelin North America
Micron Technology, Inc.
Microsoft Corporation
National Alliance for Jobs and Innovation (NAJI)
National Association of Manufacturers (NAM)
New England Council
NIKE
Pfizer
Pharmaceutical Research and Manufacturers of America (PhRMA)
Philips Lighting
The Proctor & Gamble Company
Semiconductor Industry Association (SIA)
Software and Information Industry Association (SIIA)
US Chamber of Commerce
United Technologies Corporation

Prepared with the assistance of Covington & Burling