KILPATRICK TOWNSEND

4 KEY TAKEAWAYS

International Tidbits: An Overview of Unitary Patents, Brand Protection in China, Import and Export Controls, and Compliance – Part 3

Kilpatrick Townsend recently held its annual KTIPS (Kilpatrick Townsend Intellectual Property Seminar). Firm attorneys led a day of interactive discussions with clients on the latest developments in intellectual property law and their impact on patent and trademark strategies. Kilpatrick Townsend attorneys Maria Baratta, Kristin Doyle, Adria Perez, and Gunjan Talati presented "International Tidbits: An Overview of Unitary Patents, Brand Protection in China, Import and Export Controls, and Compliance."

Ms. Perez's takeaways from the presentation include:

1

Last March, Deputy Attorney General Monaco emphasized that there is an overlap between corporate crime and national security issues: "Because in today's complex and uncertain… geopolitical environment, corporate crime and national security are overlapping to a degree never seen before, and the department is retooling to meet that challenge…."[1] She mentioned that the "retooling" includes the addition of more than 25 new prosecutors and the hiring of the National Security Division's first-ever Chief Counsel for Corporate Enforcement.

[1]U.S. DEPARTMENT OF JUSTICE, *Deputy Attorney General Lisa Monaco Delivers Remarks at American Bar Association National Institute on White Collar Crime* (March 2, 2023).

2

Intellectual property crimes that are considered national security threats include:

- Economic espionage (18 U.S.C. § 1831);
- Criminal trade secret theft (18 U.S.C. § 1832);
- Foreign influence related to research security and integrity; and
- Cyber breaches and intrusions.

3

The federal government can also leverage the False Claims Act ("FCA") against companies and institutions to mitigate the foreign influence related to research security and integrity. The FCA has been used against companies and institutions for:

- Submitting U.S. grant applications without disclosing that certain researchers had been simultaneously funded by foreign government grants;
- Providing falsified research results to U.S. government agencies to procure federal dollars; and
- Failing to comply with the federal government's cybersecurity requirements despite certifications.

Companies and institutions need a reasonable and effective compliance program to mitigate the risks from IP crimes that the government believes include national security threats. Components of such a compliance program may include:

- Conducting a risk assessment to determine how best to use company's resources to mitigate the largest compliance threats.
- Consistently training on:
  - Potential civil and criminal exposure for institutions and researchers when it comes to grant/sponsored research applications and requirements;
  - Conflict of interest and conflict of commitment requirements;
  - Data security; and
  - Related policies.
- Ensuring you document the training and attendance;
- Determining ways to enhance communication and remove silos between researchers, departments and support functions, including levels of required approvals for information provided to the government.
- Implementing security protections and requirements to decrease human error.
- Performing cybersecurity audits and cyber monitoring.

4

For more information on how to protect your company or institution against criminal trade secret theft and economic espionage, please click here for our August 2022 takeaways.

For more information, please contact:
Adria Perez: aperez@kilpatricktownsend.com

www.kilpatricktownsend.com