

## International Trade & Customs Update

March 2012

### Is Your Company's Website Revealing International Trade Law Violations?

Your company's website may be revealing international trade law violations that could result in significant civil and/or criminal penalties. Companies using their websites to conduct e-commerce or cross-border transactions involving the import or export of goods, technology or services, and/or to provide "controlled" information over the Internet or an intra-company network are particularly vulnerable to a wide range of possible violations.

To reduce your company's overall exposure, a website audit is recommended to identify information or resources on the website that may place the company at risk for violations. These risks may be limited to the website itself and how the information is presented, or they may reveal significant gaps in the company's international trade compliance program that must be addressed substantively.

Examples of potential violations revealed on a company's website include:

- A list of products available for export that may require U.S. government licensing as dual-use or defense/military items.
- A list of locations where the company conducts business that includes:
  - Countries subject to U.S. government economic sanctions.
  - Countries subject to significant U.S. government licensing requirements for dual-use or defense/military items.
  - Countries notorious for transshipping product to countries subject to such sanctions or such licensing requirements.
  - Countries the U.S. government has identified as actively promoting violations of the anti-boycott laws.
- Countries identified among the worst for corrupt public sector practices (*e.g.*, bribes).
- Reports of the company's research and development activities with foreign subsidiaries or parties that may involve controlled goods, technology or services subject to U.S. government "deemed export" licensing requirements for dual-use or defense/military items.
- Technology on the company's intra-company network accessible through the website by foreign employees subject to U.S. government "deemed export" licensing requirements or by U.S. employees located in countries subject to U.S. government dual-use or defense/military licensing requirements.
- "Made in America" product claims undermined by other website information indicating that the company imports its inputs or is selling foreign product.
- A news release announcing the company's merger with or acquisition of a foreign company with business ties to countries that require U.S. government licensing for certain exports or that face U.S. government economic sanctions.
- Evidence of website e-commerce activity or downloading between the company and parties with Internet Protocol (IP) addresses in countries subject to U.S. government economic sanctions.
- Encrypted software available for downloading from the company's website by parties in foreign countries that may be subject to U.S. government licensing for dual-use exports.

U.S. government officials or knowledgeable company whistleblowers can easily identify these potential violations on a company's website. Before these revelations become fodder for an investigation, a company should take the appropriate steps to protect itself, beginning with a website audit.

**FOR MORE INFORMATION**

For more information, please contact:

**David M. Schwartz**

202.263.4170

[David.Schwartz@ThompsonHine.com](mailto:David.Schwartz@ThompsonHine.com)

\*\*\*

*This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.*

*This document may be considered attorney advertising in some jurisdictions.*

© 2012 THOMPSON HINE LLP. ALL RIGHTS RESERVED.